능동방어

김일성종합대학출판사
주체91

능동방어

(망보안에 대한 종합해설서)

김일성종합대학출판사

이 책은 Chris Brenton 과 Cameron Hunt 가 쓴《Active Defense 》(A Comprehensive Guide To Network Security)(SYBEX Inc2001 년)을 번역한것입니다.

이 책에서는 정보보안의 필요성과 세워야 할 방책의 내용을 비롯하여 망보안을 위한 리론기술적내용에 대하여 많은 실례자료들을 서술하였으므로 이 부분 전문가들과 경영일군들(법일군들), 현직일군, 교원, 학생들에게 참고로 될수 있을것입니다.

이 책의 내용과 서술이 자본주의사회를 배경한것이므로 비판적으로 읽기 바랍니다.

차　례

머리글

제1장. 망보안의 필요성

공격자의 립장에서 생각하자 19
- 공격자, 해커, 크래커 19

왜 망을 파괴하려고 하는가 21
- 내부로부터의 공격 21
- 외부로부터의 공격 22

제1장의 조사표 26

요약 27

제2장. 얼마만한 보안이 필요한가

위험분석 28
- 어떤 자산을 보호하여야 하는가 28
- 무엇으로부터 망자원을 보호하려고 하는가 31
- 누가 망을 파괴하려고 하는가 32
- 공격의 가능성은 어떠한가 32
- 직접비용은 얼마인가 32
- 장기적회복비용은 얼마인가 33
- 어떻게 망자원을 효과적으로 보호할수 있는가 34
- 내가 관리자상급에 지배되는가 35

보안실현을 위한 예산안 세우기 35

자료들을 문서로 만들기 36

보안방책을 세우기 37
- 보안방책의 기초 37
- 훌륭한 보안방책을 세우려면 무엇이 필요한가 40
- 좋은 보안방책의 실례 44

요약 45

제3장. 망체계통신에 대한 리해

자료프레임의 해부 46

이써네트프레임 46

프레임머리부 47

통신규약이 하는 일 51

OSI모형 52

OSI모형은 어떻게 동작하는가 55

망층에 대한 보충 57

경로기 58

경로조종표 59

정적경로조종 59

거리벡토르경로조종 60

련결상태경로조종 67

접속 및 무접속형통신 69

접속형통신 69

무접속형통신 71

보안문제 73

망봉사 74

파일전송규약(FTP): 특수경우 79

다른 IP봉사 82

웃층의 통신 96

요약 97

제4장. 위상구조적인 보안

망전송에 대한 리해 98

수자식통신 98

전자기간섭(EMI) 99

빛섬유케블 101

속박 및 비속박전송 103

전송매체선택 104

위상구조적인 보안 105

이써네트 106

광지역망위상구조 108

프레임중계와 X.25 109
비동기전송방식(ATM) 111
기초적인 망련결하드웨어 112
반복기 112
집선기 112
망다리 113
교환기 116
경로기 119
망다리/교환기/경로기의 대비고찰 122
계층-3교환 122
요약 123

제5장. 방화벽

접근조종방책의 정의 124
방화벽의 정의 126
언제 방화벽이 요구되는가 126
방화벽의 류형 127
정적파케트려과 127
동적파케트려과 136
상태려과 143
대리자 143
어떤 류형의 방화벽을 리용하여야 하는가 148
동적려과 또는 대리자 148
어느 플래트홈을 선택하여야 하는가 149
봉사기에 기초한 방화벽 150
Windows 2000 155
응용기초 방화벽 155
방화벽의 기타 문제 156
주소변환 157
방화벽가입등록과 분석 160
가상사설망 162
침입검출과 응답 162
통합과 접근조종 163
제3자의 도구 164

자신이 결심하라 164
방화벽의 배비 164
요약 167

제6장. Cisco경로기의 보안특징

Cisco경로기 168
어디서 시작할것인가 169
기초적인 보안관련문제 169
사용자EXEC방식 170
특권방식 170
Cisco보안의 특징 178
접근목록의 기초 180
표준접근목록 182
정적확장접근목록 186
접근목록모임을 만들기 188
동적접근목록 190
반사적접근목록 192
TCP차단 192
문맥에 기초한 접근조종 193
방화벽침입검출체계 195
인증대리자 197
응용프로그람넘기기 199
망주소변환 200
사용자인증과 권한부여 201
보충적인 보안예방책 202
원천에서 스머프를 막기 203
바운스싸이트에서 스머프를 막기 203
목표싸이트에서 스머프를 막기 204
요약 204

제7장. Check Point의 방화벽-1

방화벽－1의 개괄 205

GUI관리대면부 205
관리봉사기 205
방화벽모듈 206
보안 및 관리봉사 207
망주소변환(NAT) 207
가상사설망(VPN) 207
가벼운 등록부접근 규약(LDAP) 208
제3자의 장치관리 208
고장극복성 208
부하균형 208
플래트홈의 선택 209
방화벽설치를 위한 NT준비 210
설치하기전의 간단한 검사 212
방화벽-1의 설치 214
방화벽-1의 구성도구 프로그람 218
방화벽-1의 보안관리 219
방화벽을 위한 객체만들기 221
NAT작업 223
방화벽-1규칙들의 동작 229
방화벽속성변경 232
보안봉사기의 동작 235
규칙들의 설치 239
요약 240

제8장. 침입검출체계

IDS에 대하여 자주 제기 되는 질문 241
IDS의 제한성 242
눈물방울공격 242
다른 알려 진 IDS의 제한성 244
IDS의 보복수단 248
호스트기초IDS 250

IDS융합 252
IDS의 설치 254
시작하기전에 254
RealSecure설치 257
RealSecure구성 260
사건감시 268
보고기능 270
요약 271

제9장. 인증과 암호화

보다 높은 보안을 위한 요구 272
평문전송 272
인증의 필요성 275
대화가로채기 275
목적지확인 276
암호화101 278
암호화방법 279
암호화부족점 281
정부의 간섭 284
좋은 암호화가 필요하다 285
해결방법 286
자료암호화규격(DES) 286
개량암호화규격(AES) 286
수자식증명서봉사기 286
IP보안 287
Kerberos 288
점대점갱도규약과 계층2 갱도규약 288
원격접근전화가입사용자 봉사(RADIUS) 289
RSA암호화 289
하쉬알고리듬 290
안전한 쉘(SSH) 290
안전한 소케트층(SSL) 291
보안통표 291
인터네트규약을 위한

단순열쇠관리(SKIP) 293

요약 293

제10장. 가상사설망

VPN기초 294

VPN의 리용 296

VPN제품의 선택항목 299

VPN제품의 종류 301

또다른 VPN 303

VPN의 설치 304

방화벽의 준비 304

VPN도식 305

필요한 망객체들의 구성 306

열쇠교환 311

보안방책의 변경 313

VPN검사 316

요약 318

제11장. 비루스, 트로이목마, 웜

비루스 :통계자료 319

비루스란 무엇인가 320

복제 320

잠복 323

폭탄 326

속이기 327

웜 328

트로이목마 331

트로이목마는 왜 비루스가 아닌가 331

바로 내가 트로이목마를 구입하였는가 331

방지방법 332

접근조종 332

검열합확인 333

과정감시 333

비루스스캐너 334
발견적스캐너 336
응용프로그람준위비루스
스캐너 337
비루스보안의 배비 337
탁상형체계의 보호 338
NT 및 NetWare봉사기의
보호 340
UNIX체계의 보호 341
요약 342

제12장. 재난방지와 회복

재난의 류형 343
망재난 344
매체 344
위상구조 346
단일고장점 352
구성파일들의 보관 354
봉사기재난 355
무정전전원(UPS) 356
저가격디스크묶음(RAID) 356
여유봉사기 359
클라스터화 360
자료의 여벌복사 360
응용프로그람봉사제공자 363
봉사기회복 364
재난의 모의 365
비파괴형검사 365
처리과정의 문서화 366
Windows 2000과 Windows
NT에서 Octopus 366
Octopus의 실례 366
Octopus의 설치 368
Octopus의 구성 370
Octopus의 검사 374
요약 376

제13장. NetWare

NetWare핵심부OS 377

C2증서 378

NetWare등록부봉사 379

NDS설계 380

구좌관리 381

식별 381

가입제한 382

통과암호제한 382

가입시간제한 383

망주소제한 384

침입자차단 384

파일과 등록부에 대한 권한 385

그룹성원 386

보안등가 386

파일체계 387

계승권한마스크 387

경과기록과 검열 389

Auditcon 389

망보안 391

파케트서명 391

Filtcfg 392

공개열쇠하부구조봉사 (PKIS) 395

Novell의 모듈인증봉사 (NMAS) 395

NetWare보안의 세부변경 397

SECURE.NCF 397

보안조종탁 398

원격조종탁접근의 보안 398

판도라인자 400

요약 401

제14장. NT와 Windows 2000

NT에 대한 개괄 402

NT령역구조 403

령역정보보관 404

령역신뢰 404

신뢰구조설계 405

사용자구좌 406

SID와 관련한 작업 407

보안구좌관리자 408

사용자관리방책구성 409

보안방책과 프로필 413

파일체계 417

허가 417

경과기록 422

사건보기의 구성 422

사건보기기록의 검사 423

체계사건의 검열 425

보안림시보수 426

리용가능한 IP봉사 427

콤퓨터열람기 427

DHCP중계국 427

Microsoft의 DHCP 봉사기 428

Microsoft의 DNS 봉사기 428

Microsoft의 인터네트정보봉사기 428

Microsoft의 TCP/IP인쇄 429

망감시기관리자 430

인터네트규약을 위한 RIP 431

RPC구성 431

간단한 TCP/IP봉사 431

SNMP봉사 431

Windows 인터네트 이름봉사(WINS) 432

Windows NT에서
파케트려과 432
파케트려과가능성 433
파케트려과구성 434
NT포구에 대하여 알아야
할 문제 436
DCOM의 보안 437
DCOM전송의 선택 437
DCOM에서 리용되는
포구들의 제한 439
DCOM과 NAT 440
Windows봉사에 리용된
포구 441
보충적인 등록고
열쇠변경 442
가입기발 442
마지막가입이름의 숨기기 443
Windows NT워크스테이션
에서 등록고보안 443
페지파일의 제거 444
Windows 2000 445
능동등록부 445
파일체계암호화 446
Kerberos Version 5 446
공개열쇠증서봉사 447
IPSec 449
스마트카드 451
요약 452

제15장. UNIX

UNIX력사 453
FreeBSD 454
Linux 455
UNIX파일체계 456
UID와 GID에 대한 리해 456
파일허가 457
구좌관리 460

통파암호파일 461
그룹파일 463
국부조종탁에로의 뿌리
가입을 제한한다 466
UNIX핵심부의 최적화 467
Make의 동작 467
망구동기설정의 변경 476
IP봉사관리 477
IP봉사 477
Inetd 483
다른 봉사와의 작업 487
TCP포장기 488
요약 489

제16장. 공격의 해부

정보수집 490
whois지령 490
Nslookup지령 492
검색엔진 495
망의 조사 496
Traceroute지령 496
호스트와 봉사의 주사 498
피동적감시 501
취약성검사 503
공격의 개시 506
숨겨진 구좌 507
중개자 507
완충기넘침 510
SYN공격 511
눈물방울공격 512
스머프 513
힘내기공격 515
물리적접근공격 516
요약 517

제17장. 공격을 앞지르기

제작자들로부터의 정보 518

3COM 518

Cisco 519

Linux 520

Microsoft 521

Novell 522

Sun Microsystems 523

제3자의 통로 524

취약성자료기지 524

Web싸이트 526

우편목록 528

뉴스그룹 530

환경검열 531

Kane보안분석기 531

요약 537

부록 1. CD-ROM에 대하여

방화벽-1(FireWall-1) 538

가디언(Guardian) 539

인터네트스캐너 (Internet Scanner) 539

망감시프로그람묶음(NMS) 540

WinZip 540

부록 2. 망리용방책의 실례

효과적인 망리용방책의 원리 541

소유총비용(TCO) 541

위험경감 541

개발과정 542
범위 543
망관리 544
통과암호에 대한 요구사항 544
비루스예방방책 545
워크스테이션여벌복사방책 545
원격망접근 546
일반적인 인터네트
접근방책 546
인터네트Web싸이트
접근방책 547
인터네트우편과 뉴스그룹
접근방책 547
개인의 인터네트구좌 547
비밀과 경과기록 548
추가정보 548
색인 549

머 리 글

망환경을 안전하게 하는것이 지금보다 매우 쉬운 과제였던 시기가 있었다. 그때에는 매개 사용자가 하나의 통과암호를 가지고 있고 정확한 파일허가준위가 설정되여 있으면 자기의 망환경이 안전하다고 생각하였다. 물론 이러한 믿음이 어떻게 증명되였는가는 알수 없지만 사람들은 그것을 그대로 믿고 망환경의 안전성에 대하여 더이상 생각하지 않았다.

그러나 인터네트가 출현하자 모든것이 변화되였다.

인터네트가 출현하자 정보의 보급속도는 급속히 증가하였다. 1990년대 초에는 보안취약성이라는 말이 주요 잡지나 신문들에 나지 않는 한 들어 볼수 없었다.그러나 그때에도 사람들이 더는 쓰지 않는 낡은 프로그람들에 대하여서는 취약성이 론의되였으나 많은 사람들은 취약성문제에 대하여 관심을 적게 돌리고 있었다. 오늘날에 와서는 많은 사람들이 1시간이 멀다하게 취약성에 대해 자주 말하게 되였다.

이것은 제품의 취약성에 대한 이 모든 론의가 나쁜것이라고 말하자는것이 아니다. 사실상 그 반대의것이 진실이다. 나쁜 의도를 가진 사람은 언제나 있었다. 저작권침해게시판은 1980년대이후 여러 곳에 있었다. 대표적으로 일부 사람들은 이러한 정보를 가장 필요로 하는 사람들 즉 안전한 환경을 유지하려고 하는 망관리자들에게 전달할 아무런 수단도 가지고 있지 못하였으며 오히려 따돌림을 당하였다.

인터네트는 안전한 환경유지에 책임 있는 사람들에게 취약성정보를 얻을수 있게 하는 훌륭한 수단으로 되였다.

망자원보안문제에 대한 인식이 높아짐에 따라 그에 대한 책임성도 커지게 되였다. 이러한 문제는 취약성을 해결하여야 하는 프로그람회사들뿐아니라 보안방책을 세우고 배비하여야 하는 망관리자나 보안전문가에 있어서도 마찬가지이다.

우편목록에 가입된 임의의 말단사용자들이 망전문가와 마찬가지로 취약성에 대하여 알게 되면서부터 보안관련문제를 배비하여야 할 절박성은 더욱 높아 졌다.

그러므로 다른 문제들에서와 마찬가지로 보안에 대하여서도 좋은 자세를 가지는것이 필요하다.

기본문제는 어디서부터 시작하는가 하는것이다. 방화벽에 대한 책을 살것인가 아니면 망봉사기보안에 대한 책을 살것인가? 이러한 취약성들이 어떻게 존재할수 있는가를 리해하기 위하여서는 망통신에 대하여서도 더많이 배워야 할것이다.

이 책의 첫 판이 출판된 다음 얻은 한가지 교훈은 보안문제를 어떤 하나의 고정된 프로그람으로서가 아니라 망과 정보기술의 모든 측면을 동반하며 끊임없이 변화되는 과정으로 보아야 한다는것이였다.

망의 어느 한 측면만 고찰하여서는 망환경의 안전을 기대할수 없다. 또한 이 과정이 다른 망조작들과 독립적으로 진행될수도 없다.

이 책에서는 체계 및 망관리자들에게 여러 측면에서 안전보호가 담보된 망을 운영하는데 필요한 정보들을 제공하며 유용성, 비밀성, 관리가능성문제들을 고찰한다.

이 책에 포함된 내용

제1장은 왜 망자원을 공격할수 있는가 하는것을 간단히 설명하는것으로 시작한다. 여러가지 종류의 공격자가 공격에 의하여 무엇을 얻으려 하는가를 배운다. 장의 마지막에 망에 대한 잠재적인 위협들의 수준을 평가할수 있는 조사표를 주었다.

제2장은 위험분석과 보안방책의 일반적개념을 준다. 위험분석의 목적은 망환경에 필요한 보안의 준위를 정량화하는것이다.

보안방책은 안전한 환경을 유지하기 위한 기관의 방책을 정의한다.

위험분석과 보안방책문서들은 보안대책을 선택하고 실현할 때 중요한 기초로 된다.

제3장에서는 망에서 체계들이 어떻게 통신하는가를 간단히 고찰한다.

이 장에서는 정보가 어떻게 포장되는가를 고찰하고 규약의 리용에 대하여 서술한다. 경로조종규약들에서의 취약성과 어느 규약이 안전한 망환경을 유지하는데 도움이 되는가를 서술한다. 마지막으로 FTP, HTTP, SMTP와 같은 봉사들을 어떻게 안전하게 리용할것인가에 대하여 설명한다.

제4장에서는 위상구조적인 보안을 취급한다. 이 장에서는 여러가지 배선형식의 보안상 우점과 약점 그리고 이써네트나 프레임중계 등 여러가지 론리적위상구조의 보안특징들을 서술한다. 또한 교환기, 경로기 그리고 계층3교환 등의 망하드웨어들을 어떻게 리용하면 보다 안전한 환경을 보장할수 있는가를 배운다.

제5장은 파케트려파기나 방화벽과 같은 경계선보안장치들에 대하여 서술한다. 접근조종방책을 세우고(2장의 보안방책에 기초하여) 각이한 방화벽방법들의 우점과 약점을 검사한다. 또한 TCP기발들과 ICMP의 형태코드와 같은 접근조종방책을 세우는데 도움이 되는 몇가지 표들을 주었다.

제6장에서는 Cisco경로기자체의 보안특징으로부터 시작하여 표준 및 확장접근목록들을 고찰한다. 파케트려파기를 리용하여 무엇을 막을수 있고 무엇을 막을수 없는가를 고찰하며 많은 접근목록실례들을 고찰하였다. 그리고 경로기를 동적파케트려파기로 동작하게 하는 Cisco의 새로운 재귀려과방법을 고찰한다.

제7장에서는 망환경에 방화벽을 어떻게 배비할것인가를 보게 된다. 특히 Check Point의 방화벽−1의 설치와 구성설정을 고찰하며 기반조작체계의 보안을 보장하고 쏘프트웨어를 설치하며 접근조종방책을 실현하는것을 고찰한다.

제8장은 침입검출체계(IDS)를 취급한다. 하나의 IDS가 감시할수 있는 자료흐름패턴 그리고 이 기술의 일부 제한성을 보게 된다. 특정한 형태의 IDS실례로서 인터네트보안체계의 RealSecure를 고찰한다. 여기서는 조작체계준비, 쏘프트웨어설치 그리고 RealSecure를 어떻게 구성설정하여 특정형태의 취약성들을 검사할것인가를 취급한다.

제9장에서는 인증과 암호화를 취급하였다. 강한 인증이 왜 중요하며 어떤 종류의 공격이 약한 인증방법들을 리용하는가를 배운다. 여러가지 암호화방법들을 취급하고 암호화를 위하여 어떻게 옳은 알고리듬과 열쇠크기를 선택할것인가 하는것을 본다.

제10장에서는 가상사설망(VPN)에 대하여 배운다. VPN의 배비가 언제 필요하며 그 배비를 위하여 어떠한 선택들이 준비되여 있는가를 고찰한다. 한가지 실례로서 두개의 FireWall−1 방화벽을 리용하여 어떻게 VPN을 만들것인가를 보게 된다. 또한 VPN이 자료흐름에서 정확히 무엇을 하는가를 알게 된다.

제11장에서는 비루스, 트로이목마, 웜에 대하여 취급한다. 이 프로그람들사이의 차이를 밝히며 정확히 그것들이 체계에서 무엇을 할수 있고 무엇을 할수 없는가를 보여 준다. 차단프로그람을 배비하기 위한 몇가지 설계실례들, 여러가지 보호방법들도 서술하였다.

제12장은 재난방지와 회복을 취급한다. 망의 여러 측면들을 고찰하면서 어디서 재난이 발생할수 있는가를 따져 본다. 광지역망에서 여분의 련결을 만드는것을 배운다. 이 장의 뒤에서 Qualix회사의 제품인 Octopus HA+의 설치와 리용을 서술한다.

제13장에서는 노벨회사의 NetWare조작체계를 서술한다. 사용자구좌설정, 파일허가 및 NDS설계를 통하여 NetWare환경을 안전하게 하는 방법들을 배우게 된다. 또한 이 조작체계에 준비되여 있는 검열기능들을 서술하였다. NetWare에 어떠한 취약성이 있으며 그것을 어떻게 대책할것인가 하는것을 보게 된다.

제14장에서는 Microsoft Windows의 망기술 특히 NT봉사기와 Windows 2000봉사기에 대하여 서술하였다. 보안기능이 강화된 령역구조설계를 취급하며 보안방책들을 어떻게 리용할것인가를 본다. 사용자구좌의 기록, 파일허용 그리고 일부 통과암호의 불확실성 등을 보여 준다. NT의 IP봉사와 그것들을 배비하는데서의 보안성문제들을 보여 준다.

제15장은 UNIX에 대하여 서술한다. 특히 Linux조작체계를 리용하는 체계를 어떻게 보안할것인가를 설명한다. 사용자구좌, 파일허가 및 IP봉사를 취급한다. 그리고 보안을 보다 강화하기 위하여 조작체계핵심부를 어떻게 재구성할것인가를 상세히 설명한다.

제16장에서는 공격자가 어떻게 정보를 수집하고 취약성들을 조사하는가 그리고 어떤 공격들이 있는가를 보여 준다. 공격자에게 있는 몇가지 쏘프트웨어도구들도 고찰한다.

제17장에서는 보안취약성에 대한 정보원천들을 소개하였다. 제품의 판매자로부터의 정보들과 많은 제3자의 자원들을 소개한다. 취약성자료기지, Web싸이트 그리고 우편목록들을 제시한다. 마지막으로 모든 망체계들이 설정한 보안방책에 추종하는가를 확인하는 도구인 Kane보안분석기를 리용하여 망환경을 검사한다.

누가 이 책을 읽어야 하는가

이 책은 보안분야에서 많은 경험을 가지고 있지 않지만 하나의 완전한 체계를 운영하려는 사람들을 위하여 특별히 계획하고 집필하였다. 만일 자기 지식기지의 마지막 5%를 마저 채우려고 하는 보안전문가라면 이 책은 그런 사람들에게는 적합하지 않다.

그러나 만일 자기의 가장 큰 약점을 알도록 하는 실천적인 차림표를 찾고 있다면 이 책은 옳은 선택으로 된다. 이 책은 전형적인 망 또는 체계관리자들을 념두에 두고 쓴것이다. 망과 봉사기의 관리사업을 하고 있으면서 보안문제로 하여 피해를 보지 않기 위한 방도를 찾고 있는 관리자들에게 적합하다.

망보안문제는 만일 시간당 350딸라의 비용으로 콤퓨터환경을 조사하고 수리하여 주는 보안전문가를 데려다 쓸수 있다면 매우 쉬운 문제일것이다. 그러나 대부분의 사람들에게 있어서 이것은 예산수준에 맞지 않는다. 강력한 보안체계는 비싸지 말아야 하지만 구체적으로 하자면 시간과 노력이 많이 든다. 망환경의 약한 고리들을 많이 보강할수록 공격자가 망에 대한 공격에서 자원을 파괴하기가 더 어려울것이다.

이 책의 내용과 관련하여 의문이 있거나 설명이 필요하다면 다음의 전자우편주소로 어느때든지 문의해 주기 바란다.

cbreton @ sover. nef 또는 cam @ cameronhunt. com

제 1 장. 망보안의 필요성

콤퓨터공격이 발생하였다는 소식이 매일같이 신문에 실리고 있다. 거의 매일 정부나 회사, 기관들이 운영하는 체계들이 침입 당하거나 파괴되였다는 소식을 듣고 있다. 심지어 미국방성과 Microsoft와 같은 높은 급의 기관들도 해킹 당하고 있다.

이러한 기관들도 공격의 희생물이 되는데 자기의 회사를 보호하기 위해 무엇을 할수 있겠는가를 생각할수 있다.

보다 나쁜것은 대부분의 공격들이 공개되지 않는다는것이다. 미련방수사국에 대한 공격은 신문의 첫 페지에 실리지만 많은 낮은 급의 기관들에 대한 공격들은 일반대중에게는 알려 지지도 않는다. 어느 회사가 자기의 금융정보를 가지고 있다든가 또는 최신제품의 설계를 도난 당했다든가 하는것이 일반대중에게 알려 지면 엄중한 경제적손실을 일으킬수 있다. 실례로 어느 은행이 자기의 콤퓨터보안이 침해 당하고 많은 량의 돈이 잃어 졌다고 공개한다면 어떤 현상이 생기겠는가를 보자. 이 은행에 구좌를 가지고 있다면 그는 무엇을 할것인가? 명백히 은행은 이 사건을 조용히 덮어버리려 할것이다.

완전히 등록되지 않은 많은 공격들이 있을수 있다.

가장 일반적인것은 내부적공격인데 이러한 경우에 회사나 기관은 그 종업원을 해고하는것 이상으로 문제를 확대하지는 않을수 있다. 실례로 한 박물관에서 자기들의 현재의 망설정을 보아 달라고 보안전문가에게 물어 본적이 있었다. 박물관책임자는 망담당자들이 어떤 부정적인 활동에 참가하고 있다고 의심하고 있었다.

보안전문가는 망담당자들이 모든 사용자들의 우편함(책임자의것도 포함하여), 로임자료기지 그리고 기부자자료기지에 침투하였다는것을 알아 냈다. 그들은 또한 박물관의 자원을 리용하여 자기들의 기업을 운영하고 있었으며 다른 망들을 공격하는데 리용될수 있는 프로그람도구들을 퍼뜨리고 있었다. 이러한 침해에도 불구하고 박물관에서는 법적제재없이 그들을 그저 해고시키기로 하였다. 일단 해고되자 그들은 자기들을 위하여 망에 설치한 많은 《뒤문》들을 리용하려고 하였다. 계속되는 이러한 행위들이 탄로났으나 박물관에서는 그것을 일반에 알려 지기를 바라지 않았다.

얼마나 많은 보안관련사건들이 등록되지 않고 있는가에 대한 명백한 통계자료는 없다. 경험에 의하면 사실상 대부분이 등록되지 않는다고 말할수 있다. 명백히 보안침해는 계속 발생하고 있고 매개 망은 공격을 막기 위한 전략적대책을 요구한다.

기본내용에 들어 가기전에 다음과 같은 문제에 대하여 보기로 하자. 먼저 누가, 왜 망을 공격하려 하는가 하는것을 보려고 한다.

공격자의 립장에서 생각하자

어떻게 하면 자원을 가장 잘 지킬것인가를 결정하기 위하여서는 누가 그것을 파괴하려고 하는가를 알아야 한다.

대부분의 공격들은 우연적인것으로 볼수 없다. 공격을 계획하는 사람은 공격대상자의 자산을 혼란시킴으로써 무엇인가 얻는것이 있다고 본다. 실례로 도적은 부자들을 더 털어 내고 싶어 하는것이다. 누가 자원을 훔치거나 혼란시킴으로써 리득을 얻으려고 하는가를 아는것이 그것을 보호하기 위한 첫 단계로 된다.

공격자, 해커, 크래커

많은 사람들은 흔히 공격자, 해커, 크래커라는 말을 같은것으로 쓰고 있다. 《우리는 해킹 당했다.》라는 말은 《우리는 공격 당했다.》는 말과 같은 의미를 가지는것으로 보고 있다.

그러나 이 세개의 용어는 큰 차이를 가지고 있으며 그 차이를 리해하여야 누가 망의 보안을 돕고 누가 그것에 침입하려고 하는가를 알수 있다.

공격자는 대상자의 자원을 훔치거나 혼란시키려 하는 사람이다. 공격자는 기술적으로 전문가이거나 수준이 높은 애호가일수 있다. 공격자는 간첩이나 도적과 비슷하다.

해커의 원래 의미는 콤퓨터와 망에 대한 깊은 지식을 가지고 있는 사람이다. 해커들은 프로그람이나 간단히 실행시키는것에 만족하지 않으며 그것이 어떻게 동작하는가 하는 구체적인 특성까지 다 알려고 한다. 해커는 명백한것 이상으로 알아야 할 필요를 느끼는 사람이다. 해킹기술은 그의 사람됨과 동기에 따라 긍정적일수도 있고 부정적일수도 있다.

해킹은 그들자신의 부문문화와 자신의 언어 그리고 인정된 사회적실천을 가지고 있다. 해커를 공격자나 지어 무정부주의자로 보도록 사람들을 추동하는것이 아마도 사람들의 습성인것 같다.

력사에는 그 시대의 문화수준의 리해를 훨씬 초월한 사람들이 많이 있었다. 레오나르도 다 빈치, 갈릴레오, 바이론, 모짜르트, 테슬라 등은 모두 《공인된 사회적표준》과는 맞지 않는 《이상한》사람들로 인정되여 있었다.

정보시대에 와서는 이런 역할을 해커라고 부르는 사람들이 하고 있다고 볼수 있다.

해커들은 보통 주장을 그대로 받아 들이지 않는다. 실례로 한 판매자가 《우리 제품은 100% 안전하다.》라고 주장하면 해커는 그것을 하나의 도전으로 여길수 있다.

해커가 알려 진 정보를 가지고 무엇을 하는가 하는것을 보면 그 해커가 어떤 색갈의 모자를 썼는가를 결정할수 있다.

어떤 정보체계에 대하여 리해를 더 하려고 하는 해커들과 그 지식을 리용하여 체계에 비법적 또는 비도덕적으로 침투하려 하는 해커들사이를 구별하기 위하여 콤퓨터부분의 일부 사람들은 후자를 가리켜 《크래커》(Cracker)라는 용어를 쓴다. 이것은 《해커》라는 용어의 전통적인 의미를 보존하려는 시도였지만 이러한 시도는 크게 성과를 보

지 못하였다. 출판물들까지도 때로 그 용어를 쓰고 있다.

그러나 법률은 그 의도에서의 차이를 인정하지 않으며 다만 비법적으로 체계에 침입한 행위로 본다.

흰모자해커, 회색모자해커, 검은모자해커

어떤 프로그람에서 보안상의 약점을 리용할 방법을 얻은 해커와 그 약점을 공개하여 알려 지게 하려는 해커를 흰모자해커라고 부른다.

그러나 만일 해커가 보안상의 약점을 발견하고 자기의 개인적리익을 위하여 그것을 리용하려고 한다면 그 해커는 검은 모자를 쓰고 있다고 한다.

회색모자해커는 낮에는 흰 모자, 밤에는 검은 모자를 쓰는 해커이다. 달리 말하면 보통 합법적인 보안전문가로 일하지만 자기시간에는 비법적인 활동을 계속하는 해커이다.

회색모자로 볼수 있는 한 사람의 실례를 보자.

J라는 보안문제상담자가 한 조작체계의 불안전한 뒤문을 하나 발견하였다.

그는 그것을 공격에 리용하지는 않지만 이 공격에 대하여 자기 의뢰자의 체계를 안전하게 하기 위한 합법적인 보수를 요구한다. 달리 말하면 그는 그런 약점을 그자체로 리용하지는 않으면서 자기의 개인적리익을 위하여 그것을 리용하고 있는것이다. 결과적으로 그는 약점은 그대로 남겨 두고 그것을 막기 위한 돈을 요구하는것이다. J는 이 문제에서 공개적인 수리정비를 위하여 제작자와 협동하지 않는다. 그것은 제작자가 수리하지 않도록 하는것이 그의 관심이기때문이다.

좀더 복잡한 문제로 되는것은 많은 사람들이 보안약점의 세부를 공개하는 사람들의 동기를 오해하는것이다.

사람들은 흔히 이 사람들이 이러한 취약점들을 공개함으로써 다른 공격자들을 교육하려고 한다고 가정한다. 이것은 진실에 가까울수도 있다. 취약성정보를 일반에 공개하는것은 제작자와 체계관리자들을 경고하여 그들이 그것을 처리할 필요를 느끼게 한다. 그러나 공개적발표는 흔히 필요성과 관계없이 진행된다.

실례로 펜티움이 인텔회사의 최신제품으로 나타났을 때 사용자들은 그 소편의 수값처리기부분에서 계산오차를 가져 오는 하나의 오유를 발견하였다. 이 문제가 처음 발견되였을 때 많은 사람들은 인텔과 직접 접촉하여 그 문제를 알리려고 하였다. 그러나 그들의 주장은 거절되거나 랭담한 대접을 받았다.

오유의 세부가 인터네트를 통하여 발표되고 공개연단들에서 론의되였을 때에야 인텔회사는 그 문제를 해결하기 위한 대책을 취하였다. 결국 인텔은 자기의 소편들을 무상으로 교체해 주기로 하였으나 인텔에 대한 불만은 계속 제기되였다.

오유들과 약점들을 공개적으로 발표하는것은 문제를 해결하기 위한 좋은 방법의 하나로 될수 있다.

주　의

문제가 생기면 먼저 제품제작자에게 알리고 수정이 진행될 때까지 공개하지 않는것이 옳은 례절이다. 보통은 제작자에게 적어도 두주일의 시간을 주고 공개연단에서 약점을 발표하기전에 그것을 수정하도록 한다.

대부분의 제작자들은 이러한 문제에서 매우 책임적이다. 실례로 Microsoft회사는 보안관련문제들을 그것이 알려 져서 며칠안으로 대책하고 있다. 일단 약점이 대중에게 알려 지면 대부분의 제작자들은 그 문제를 될수록 빨리 해결하려고 할것이다.

이러한 문제들의 공개적인 발표는 일부 사람들에게는 나쁜 생각을 할수 있게 하였다. 어떤 사람이 보안관련문제를 발견하고 그것을 상세히 발표하면 다른 사람들은 그가 그 보안약점을 개인적리익을 위하여 리용하고 있는 공격자라고 생각할수 있다.

그러나 보안관련문제를 론의하는데서 이러한 공개성은 쏘프트웨어제품의 안전성을 높이는데 도움을 주었다.

왜 망을 파괴하려고 하는가

그러면 무엇이 망을 공격하도록 추동하는가? 언급한바와 같이 이 공격들이 우연적인 것은 극히 드물다. 그들은 거의 항상 그 공격에 의하여 무엇인가를 얻으려고 한다. 그 공격을 유발시키는것은 회사나 기관과 그 공격을 계획하는 사람에게 달려 있다.

내부로부터의 공격

실례들을 연구한데 의하면 공격의 대부분은 회사나 기관의 내부에 근원을 두고 있다. 어떤 연구에 의하면 공격의 70%가 회사나 기관안의 사람 또는 내부의 정보를 아는 사람(해고자 등)에 의하여 진행되였다. 외부의 공격으로부터 자원을 보호하는데는 보통 방화벽을 리용하면 되지만 이것은 회사나 기관의 망이 어떻게 동작하는가 하는것을 내부적으로 알고 있으며 자료를 손상시킬수 있는 기회가 가장 많은 내부종업원에 관한 문제이다.

이 침해는 우연적일수도 있으며(사용자오유에서처럼) 또는 어떤 경우에는 의도적일수도 있다.

진짜공격의 가장 대표적인 근원은 불만을 가진 종업원 또는 해고된 종업원이다.

어떤 보안전문가가 한 새로운 의뢰자로부터 긴급호출을 받은적이 있는데 그 의뢰자는 인터네트접속을 완전히 잃었었다. 그 회사는 연구회사였으므로 인터네트가 절실히 필요했다.

그 회사는 한 종업원을 《다른 기회를 찾아 이동하도록》하는 결정을 내렸는데 그 종업원은 원래 떠나기를 원치 않았다. 그 종업원에게 자기 짐을 가지고 조용히 회사를 떠나도록 지시하였다. 작은 회사였으므로 그가 문을 나설 때까지 바래줄 필요를 느끼지 않았다.

나가는 도중에 그 종업원은 회사의 방화벽프로그람을 돌리는 UNIX체계에 잠간 멈추어 섰다. 체계는 열린채로 있었고 어떤 형태의 통과암호도 리용하지 않았다. 그는 간단한 작별인사를 남기기로 하고 여러 프로그람파일들을 모두 지워 버리였다. 그리고 경로조종기의 V.34케블을 걷어서 가까이 있는 책상에 숨기였다. 이 사건은 설비가 자물쇠로 잠근 방에 있었다면 예방할수도 있는것이였다.

대부분의 관리자들은 자기 방을 외부적공격으로부터 보호하는데는 큰 관심을 돌리지

만 내부적공격의 보다 큰 위협에 대해서는 흔히 크게 느끼지 못하고 있다.

실례로 한 회사소유자가 회사의 NetWare봉사기에 대한 완전한 감독권한을 가질것을 고집하였다. 그는 특별히 콤퓨터지식이 있는것도 아니고 이러한 접근준위를 요구하지도 않았으나 자기가 회사의 소유자라고 하여 그것을 고집하였다.

무슨 일이 일어 났는가를 독자들이 추측하리라고 믿는다. 자기의 체계에서 간단한 몇가지 조작을 하다가 그는 부주의로 자기의 M:구동기의 CCDATA등록부를 지워 버리였다. 만일 CC:Mail을 관리해 보았다면 이 등록부가 우편국을 위한 보관장소이며 모든 우편통보문들과 공개폴더들을 포함한다는것을 알았을것이다.

CC:Mail에서 기본우편파일들은 거의 항상 열려 있으며 보통방법으로는 복제하기 어렵다. 이 회사는 종업원들이 거의 쓰지 않는 개인용폴더들을 제외한 모든 우편통보문들을 잃었다. 약 2년간의 자료가 모두 없어 지고 말았다. 이것은 고의적인 공격은 아니였지만 회사의 돈을 적지 않게 소비하게 하였다.

계속 증가되는 위협은 자료의 파괴가 아니라 자료의 도난과 손상이다. 이것을 보통 산업(또는 기업)정탐이라고 하는데 내부적자료파괴와 같은것으로는 보지 않지만 독점적이며 비밀적인 정보를 가지고 있는 회사들 특히 그 자료가 손상되면 법적책임을 져야 하는 그런 회사나 기관들에서 실제적인 위협으로 된다.

이에 대한 한가지 실례는 건강보험회사(HIPAA)의 관할하에서 건강관리에 관계하는 기관을 들수 있다. HIPAA의 행정적통제밑에서 개인의 건강정보를 보호하도록 보안표준들이 설정되여 이 정보에 대한 적당한 접근과 리용이 허가된다.

비밀성에 대한 어떠한 침해도 정부의 법적제재를 받게 된다.

외부로부터의 공격

외부로부터의 공격은 많은 원천들을 가지고 있다. 이 공격들은 불만을 품은 종업원들로부터 올수도 있지만 가능한 공격자들의 범위는 많아 진다. 공통적인것은 공격에 의하여 무엇인가 얻으려 한다는것이다.

경쟁자

만일 어떤 회사가 경쟁이 매우 심한 기업을 하고 있다면 야심적인 경쟁자가 그 망을 공격하여 리득을 볼수 있다. 여기에는 설계나 금융자료를 훔치는 형태이거나 또는 망자원을 쓸수 없게 만드는것일수도 있다.

경쟁자의 설계를 훔치는것의 리득은 명백하다. 이 정보를 가지면 훔친 자는 그 회사의 설계를 리용하여 개발시간을 단축하거나 자기 제품의 성능을 더 좋게 할수 있다. 만일 경쟁자가 그 회사가 가까운 장래에 어떤 제품을 내놓는가를 안다면 그 경쟁자는 보다 인기 있는 제품으로 시장에서 그 회사를 패배시킬수 있다.

금융정보도난도 매우 불리할수 있다. 경쟁자는 회사의 완전한 회계내용을 알게 되며 시장에서 부당한 우세를 차지하게 된다. 이러한 부당한 우세는 그 회사의 재정형편에 대한 내부적시각을 가지며 회사의 수입원천을 아는데 있다.

실례로 경쟁자의 망에 침투하여 그 회사의 자산원천을 보여 주는 회계문건을 훔쳐낸 한 콤퓨터상담회사에 대하여 보기로 하자. 공격자는 특히 자산의 60%이상이 팍스기계, 인쇄기, 복사기의 판매로부터 생긴다는데 관심을 돌렸다. 이 정보를 알고 도적은 고객싸이트에 가서 말하였다. 《당신은 자기의 콤퓨터망때문에 X회사에 의존하려고 하는가? 그 회사는 주로 사무기계회사이고 그들의 기업은 팍스나 복사기를 팔고 있다.》 이러한 방법으로 그는 다른 많은 고객들에 대해서도 승리하게 되였다.

때로 공격자가 리익을 위하여 무엇을 제거하지 않아도 되는 때가 있다.

실례로 한 사람이 Web싸이트를 통하여 판매를 실현하는 한 상업회사에서 일한다고 하자. 그 사람은 자기의 목록체계를 가지고 있고 고객은 안전한 형식으로 주문을 할수 있다. 그는 자기의 특정의 시장분야에 대하여 최저가격을 준비하고 있다.

이제 한 경쟁자가 있는데 그의 가격은 약간 높다고 가정하자. 만일 경쟁자가 그의 Web싸이트를 기본련결들로부터 허용중지시킨다면 그것은 그 경쟁자의 기업에 도움이 될것이다. 그의 Web싸이트에 도달할수 없는 고객들은 대신에 경쟁자의것을 조사해 보게 될것이다. 고객들은 가격을 비교할수 없으므로 경쟁자의 싸이트에 제품을 주문하게 될것이다.

실제적인 도난은 일어 나지 않았지만 이러한 봉사거절은 직접적으로 자산을 잃게 한다. 이러한 형태의 공격은 립증하기 어려울뿐아니라 량적으로 취급하기는 보다 어렵다. Web싸이트가 8시간동안 단절되여 있다면 얼마나 많은 판매량이 잃어 졌는지 알수 있는가?

이처럼 경쟁자의 공격을 당하기 얼마나 쉬운가 하는것은 그의 기업이 얼마나 경쟁적인가 하는것과 직접 관계된다.

실례로 고등학교는 경쟁자학교가 다음학년도 과정안의 복사본을 훔쳐 가는것을 걱정하지 않아도 된다. 그러나 고등학교는 내부적공격들에 대하여 평균수준보다 더 높은 관심을 돌려야 한다.

호전적인 공격

만일 어떤 회사가 내부론쟁이 많은것으로 인정되면 그 회사는 다른 견해를 가지는 사람들로부터 침해 당하기 쉽다.

실례로 의학연구에 대한 정보를 출판하는 한 회사의 사건을 보기로 하자. 그 회사의 Web싸이트에는 류산에 대한 자료들이 들어 있었는데 그 싸이트를 검색하던 한 사람이 Web봉사기관리자에게 전자우편으로 알리기를 그 싸이트의 일부 자료들이 그 회사가 의도하는것들이 아니라고 하였다. 관리자는 류산에 대하여 서술한 모든 페지들이 류산을 반대하는 구호들과 성서인용문들로 교체된것을 발견하였다.

이러한 공격은 회색적인것으로서 정보를 도난 당하지는 않았으므로 공격자를 기소하기는 어려울것이다. 그 시기의 관련법에서는 이 공격을 비문화적행위로 규정하였다.

그러나 시대는 변하고 있다.

높은 급의 보안침해는 큰 보도거리가 되고 세계의 활동가들은 이것을 리용하여 자기

들의 목적을 추구하고 있다.

그 첫 형태는 싸이버세계에서 군사적 또는 폭력적투쟁을 하고 있는 실지로 호전적인 해커이다.

여기에 4가지의 잘 알려 진 실례들이 있다.

- 1998년 봄에 많은 관측자들은 파키스탄과 인디아가 무력적위협으로서 핵무기를 시험하고 언론전에 착수한것을 보았다. 이때 파키스탄과 인디아의 해커들은 상대방의 Web싸이트들에 대한 공격을 서로 개시하였다.
- 1999년 봄에 나토가 쎄르비아를 폭격하는 기간 쎄르비아와 알바니아해커들은 서로 상대방의 싸이트들에 침입하였다.
- 2000년에 이스라엘의 정부당국자가 팔레스티나의 성지를 방문한후에 발생한 격렬한 실제적인 적대행위들을 방불케 하는 싸이버전쟁이 팔레스티나와 이스라엘의 해커들(두 집단은 대체로 미국에 있었다.)사이에서 벌어 졌다.
- 대만과 중국의 해커들은 낮은 수준에서 여러해동안 싸이버공간에서 서로 상대방을 헐뜯고 깎아 내리였다. 어느쪽이나 다 대만섬에 대한 합법적인 주장을 가지고 있었다.

다른 형태는 보통 욕심이나 호전적인것과는 다른것들인데 흔히 《해커주의자》라고 한다. 이들은 봉사를 중지시키고 Web싸이트를 헐뜯으며 또는 자기들의 주장에 주의를 돌리게 할 목적을 가지고 체계들을 공격한다.

최근의 실례들을 보면 다음과 같다.

- 2000년 11월 7일에(미국에서 대통령선거날) 한 해커가 공화당의 민족위원회 페지에 침입하여 그 내용을 부대통령 고어의 서명들로 바꾸어 놓았다.
- 2000년 6월에 S11이라는 오스트랄리아의 한 집단이 Nike.com을 가로채서 나이크로 가려던 방문자들을 S11의 반나이크싸이트에로 보내였다.
- 1999년의 세계무역기구회의기간에 영국에 있는 전자히피라는 한 집단이 WTO의 싸이트를 일시 마비시켰다.

높은 급의 공격

잘 알려 져 있거나 대중의 눈에 자주 보이는 기관들은 그저 눈에 띄인다는것으로 하여 공격의 대상으로 될수 있다. 해커가 되보려고 하는 사람은 성과적인 공격이 자기의 이름을 높여 주리라는 희망을 가지고 이름 있는 싸이트에 침입하려고 할수 있다. 지난 몇년동안 발생한 높은 급의 공격의 실례들을 들어 보자.

- 1997년 3월에 H4G1S라고 부르는 한 집단이 미항공우주국 (NASA) 의 Web페지들중 하나를 로출시키고 그것을 인터네트를 상업화하려는 회사들에 대한 앞

으로의 공격을 경고하는 연단으로 리용하였다.

- 1999년 3월에 주요 미국정부싸이트들인 Whitehouse.gov, FBI.gov, Senate.gov들이 지워 졌다.
- 2000년 2월에 가장 높은 급의 인터네트관련회사들중 일부가 봉사거부공격을 받았다. 그중에는 Amazon.com, Buy.com, CNN.com, eBay, E*Trade, Yahoo! 그리고 ZDNet가 들어 있다.
- Microsoft는 2000년 10월에 해커들이 여러주동안 자기들의 싸이트에 침입하였다고 발표하였다. Microsoft는 해커들을 처음부터 알고 있었다고 주장하였지만 그것은 그 회사에 있어서는 굴욕적인 순간이였다.

회사나 기관이 높은 급인가 아닌가를 결정하기는 어려울수 있다. 대부분의 회사나 기관들은 인터네트에서의 자기들의 위상이나 존재를 흔히 과대평가한다. 회사가 다국적기업이 아닌 이상 또는 싸이트가 매일매일 인기 있는 Web봉사를 하지 않는 이상 그 싸이트는 아마 주요공격목표로는 되지 않을것이다.

바운스우편

가장 참을수 없는 공격형태는 자기 령역의 우편체계가 스팸중계기로 리용되는것이다. 스팸이란 무차별적인 광고배포를 의미한다. 스팸은 어떤 제품이나 봉사에 대한 관심을 불러 일으키기 위하여 무차별적으로 광고들을 배포한다. 스팸으로 하나의 광고를 발송하면 그것은 수천개의 전자우편주소들과 우편목록들에 도달하게 된다. 스팸이 어떤 우편체계를 스팸중계기로 리용하면 그 우편체계는 이 모든 통보문들을 배달하는 호스트로 된다.

그 결과는 봉사의 거부이다. 그 우편봉사기가 이 스팸우편들을 처리하는데 시간을 다 보내므로 자기의 령역(domain)에서의 합법적인 우편물들을 처리할수 없게 된다.

일러두기

가장 현대적인 우편체계는 지금 반스팸설정기능을 가지고 있다. 이 설정은 스팸통보문을 받는것을 막을수는 없으나 그 체계가 스팸중계기로 리용되지 못하게 한다.

보복을 두려워 하는 대부분의 스팸사용자들은 자기것이 아니라 남의 우편체계를 리용하려고 한다. 전형적인 스팸사용자는 실제적인 귀환주소를 숨김으로써 그 통보문을 추적하려고 하는 사람이 그것을 다른 령역에서 배포하는것으로 알게 한다. 많은 인터네트사용자들이 스팸우편을 받는것을 좋아 하지 않으므로 그들은 이 모든것을 힘들게 한다. 《달가와 하지 않아도 된다.》는것이 그들의 속대사이다. 스팸우편은 많은 사람들을 격분시키며 그들은 우편폭탄이나 봉사거부공격으로써 보복조치를 취하게 된다.

이러한 반공격은 그 기업에 인차 파괴적인 결과를 가져다 줄수 있다. 실례로 한 작

은 망제품제작회사에서 인터네트접속이 된후에 한 적극적인 판매원이 망에 련결된 매 우편목록과 뉴스그룹들에 대량우편을 보낼 좋은 생각을 하였다.

우편에서는 아주 적은 응답이 나타나는데 그 판매원이 희망했던 형태에서는 그렇지 않았다. 몇시간내로 수만개의 통보문들이 그 령역에로 배포되기를 시도하였다. 우편이 너무 많아서 우편봉사기와 우편중계기의 디스크공간이 넘쳐 나게 되였다. 수천개의 통보문속에서 어느것이 합법적인것이고 어느것이 공격을 위한것인지 결정하는것이 불가능하게 되였다. 결과로 모든 내부우편들은 쫓겨 나게 되였고 우편중계기는 공격이 가라앉을 때까지 약 한주일동안 정지되게 되였다.

이 특수한 공격은 한 종업원의 근시안적인 생각에 의한것이지만 체계를 통하여 경로설정된 외부적스팸은 같은 현상과 비용손실을 일으킬수 있다.

제1장의 조사표

아래의 내용들로부터 자기 망의 공격감수성을 평가할수 있다.

공격잠재력을 평가하기

다음의 문제들은 자기의 망에 대한 잠재적위협들을 평가하는데 도움이 될것이다. 매개 문제를 1∼5까지의 척도로 평가하시오. 1은 그 질문이 자기의 망환경에 적용되지 않는다는것을 표시하며 5는 그 질문이 직접 적용가능하다는것을 의미한다.

문제 1. 망이 도서관이나 정부기관과 같은 공공기관에 물리적으로 접근가능한가?

문제 2. 망에 학교나 대학과 같이 그 기관에 속하지 않는 사용자들이 접근가능한가?

문제 3. 인터네트봉사제공자와 같이 공개적인 망봉사를 제공하는가?

문제 4. 망담당자외에 뿌리권한 또는 관리자권한을 가진 사용자가 있는가

문제 5. 사용자에게 손님(Guest)과 같은 공통가입이름이 허용되여 있는가?

문제 6. 그 기관이 분쟁이 많은것으로 간주될수 있는가?

문제 7. 그 기관이 금융 또는 화폐정보를 취급하는가?

문제 8. 망의 일부가 일반(Web봉사기, 우편봉사기 등)에서 전자적으로 접근가능한가?

문제 9. 그 기관이 제품을 생산하는가 또는 기술봉사를 하는가?

문제 10. 그 기관이 급격히 성장하고 있는가?

문제 11. 그 기관에 대한 소식이 신문이나 상업잡지들에 정기적으로 나타나는가?

문제 12. 그 기관이 인터네트나 프레임중계와 같은 공공망통로로 기업을 하고 있는가?

문제 1－6에 대하여 자기의 기관이 8부터 12사이의 점수를 받았다면 내부망을 안전하게 하기 위한 대책을 세워야 한다. 12이상의 점수를 받았다면 내부환경을 닫아 매고 망파라메터들을 안전하게 하여야 한다.

문제 6－11에 대하여 점수가 7부터 10사이에 있다면 망은 최소의 보안으로 가장 큰 효과를 얻을수 있다. 점수가 11부터 16사이에 있다면 강력한 방화벽기술을 사용하여야 한다. 16이상의 점수라면 여러 겹의 방화벽리용을 고려하여야 한다.

주 의

이 조사표의 결과와 함께 기관안에서의 콤퓨터전문기술수준을 잘 알아야 한다.《고급한 사용자》환경은 부주의로 손해를 끼칠 가능성은 적지만 공격에 필요한 지식을 가지게 되므로 내부공격위협이 존재한다. 반대로《저급한 사용자》환경은 공격가능성은 적지만 우연적인 손해를 끼칠 가능성이 있다.

요 약

이 장에서 우리는 보안관련사건들이 계속 많아 지고 있으며 그 대부분이 공개되지 않는다는것을 보았다. 또한 해커와 공격자의 차이가 무엇이며 보안취약성문제를 공개연단에서 토의하는것이 좋다는것을 알았다. 또한 누가, 왜 망을 공격하려고 하는가, 망이 공격목표로 될수 있는 가능성은 어떠한가에 대한 평가문제를 보았다.

이제는 누가, 왜 망을 공격하려고 하는가를 리해할수 있고 회사나 기관에 대한 여러가지 위험준위도를 평가할수 있다. 위험분석을 진행함으로써 자기의 기관을 보호하는데 얼마만한 보안이 필요한가 하는것을 보다 명백히 알게 될것이다.

제2장. 얼마만한 보안이 필요한가

어떻게 하면 자기의 망을 잘 지킬것인가를 결정하기전에 달성하려고 하는 보호의 수준을 알아야 한다. 실지로 얼마만한 수준의 방어요새를 구축해야 하는가를 결정하기 위하여 망을 분석하는것으로부터 시작한다.

다음으로 이 지식을 리용하여 자기의 보안방책을 작성한다. 이 정보로 무장하면 자기의 보안구조에 대한 정확한 결정을 내리는데서 좋은 출발위치에 섰다고 볼수 있다.

위 험 분 석

위험분석이란 보호하려고 하는 자산과 그것들에 대한 적대적인 위협들을 식별하는 과정이다.

정확한 위험분석을 진행하는것은 망환경을 안전하게 하는데서 절대적으로 필요한 단계이다.

위험분석은 다음의 문제들에 대한 대답이다.

- 어떤 자산을 보호하여야 하는가?
- 어떤 공격으로부터 이 자산들을 보호하려고 하는가?
- 누가 망을 손상시키려 하며 무엇을 얻으려 하는가?
- 망에 대한 공격위협가능성은 어떠한가?
- 자산이 손상된다면 직접적인 비용손실은 얼마인가?
- 공격이나 오유를 회복하는데 드는 비용은 얼마인가?
- 어떻게 효과적인 비용으로 이 자산들을 보호할수 있는가?
- 안전한 환경을 위하여 요구되는 보안준위를 지시하는 관리자상급에게 내가 지배되는가?

어떤 자산을 보호하여야 하는가

효과적인 위험분석을 진행하려면 보호하려고 하는 자산과 자원을 아는것으로부터 시작하여야 한다. 자산은 다음의 4가지 부류로 가를수 있다.

- 물리적자원
- 지적자원
- 시간자원
- 인식자원

물리적자원

물리적자원이란 물리적형태를 가지는 자산이다. 여기에는 워크스테이션, 봉사기, 말단기, 망집선기 그리고 주변장치 등이 포함된다.

기본적으로 물리적형태를 가지는 임의의 콤퓨터자원들을 물리적자원으로 볼수 있다.

위험분석을 할 때 물리적자원을 잊지 말아야 한다.

보안방책이 엄격하지 못한 한 회사에서 있은 실례를 들어 보자.

어느 날 한 사람이 앞문으로 들어 와서 자기를 인쇄기수리공이라고 소개하였다. 접수원은 사람을 잘 믿는 사람이였는데 손을 흔들어 그를 통과시키면서 회사의 망관리자의 사무실을 가리켜 주었다. 몇분후에 그 《수리공》이 돌아 나왔는데 인쇄기가 고장나서 그것을 상점에 도로 가져 간다고 하였다.

물론 인쇄기는 고장나지 않았고 그 《수리공》은 망관리자를 찾지도 않았다. 그는 최고급의 인쇄기를 가지고 문밖으로 사라져 버렸다. 망관리자는 종업원들이 인쇄를 할수 없다고 알려서야 그 도난사고를 알게 되였다.

위험분석의 최종목적은 자원을 지키기 위한 효과적인 계획을 작성하는것이다.

분석과정에 가장 명백한 문제들을 놓치지 말아야 한다. 실례로 우에서 본 인쇄기도난사고는 회사가 모든 외부인원들을 바래주도록 요구했더라면 완전히 막을수 있는것이였다. 이러한 예방조치를 실현하는데는 비용이 들지도 않는다.

지적자원

지적자원은 주로 전자적형태로 존재하므로 물리적자원보다 식별하기가 어렵다. 지적자원은 기업에서 일정한 역할을 노는 임의의 형태의 정보일수 있다. 여기에는 프로그람, 금융정보, 자료기지, 설계도면 등이 포함된다.

때문에 시간을 들여서 지적자원들의 목록을 만들어야 한다. 여기서는 가장 명백한 대상도 잊고 빠뜨리기 쉽다. 실례로 회사가 전자우편을 통하여 정보를 교환한다면 이 전자우편통보들이 보관된 파일은 지적자원으로 보아야 한다.

시간자원

시간은 때로 위험분석에서 잊고 넘어 가는데 시간도 중요한 자원이라고 볼수 있다.

잃은 시간으로 하여 지불된 비용을 계산할 때에는 잃은 시간으로 인한 손실들을 모두 포함시켜야 한다.

잃은 시간이 얼마만한 가치가 있는가?

한가지 실례로 봉사기 한대를 기관의 자원으로 본다고 하자. 사람들은 물리적자원(봉사기자체)과 지적자원(봉사기의 하드구동기에 보관된 자료)을 같은것으로 보고 있다.

시간자원은 위험분석에서 어떻게 고려할것인가?

봉사기는 밤마다 여벌복사(back up)되고 있지만 고장은 없다고 가정하자. 모든 기술자료들을 보관한 하나의 디스크가 있다. 봉사기의 하드구동기가 고장나면 어떻게 될것인가? 이 고장으로 하여 물리적자원, 지적자원, 시간자원에서 무엇을 잃게 되는가?

물리적손실은 구동기 그자체일것이고 그 값은 얼마되지 않는다.

지적손실을 보면 마지막복사후에 구동기에 보관된 자료는 없어 질것이다. 밤마다 복사를 하므로 그 손실은 하루의 정보가치보다는 클수 없다. 시간에로 돌아 가보면 기술자들이 잃어 진 정보를 복구하는데 시간을 소비하게 된다.

실제적인 시간손실을 계산하는데서 봉사기관리자의 대수리작업을 고려하여야 한다.

봉사기관리자는

- 적당한 교체용구동기를 마련하며
- 체계에 새 구동기를 설치하며
- 필요하다면 망조작체계를 완전히 재설치하고 필요한 프로그람들도 재설치하고 여벌복사하며
- 모든 필요한 여벌복사테프들을 다시 보관하고 매일밤 완전여벌복사가 수행되지 않는다면 재보관할 테프들을 다중으로 준비하며
- 디스크공간문제들을 처리한다.

또한 봉사기관리자는 봉사기를 회복하는데만 집중하기때문에 그밖에 다른 일감들은 뒤로 미루어야 한다. 봉사기관리자가 이 모든 일들을 하고 있는 동안 기술직원들은 봉사기가 회복되기를 기다리면서 한가히 앉아 있게 된다. 결국 시간을 잃은것은 봉사기관리자뿐이 아니라 전체 기술직원들이다.

이 손실을 량적으로 표현하기 위하여 비용으로 계산해 보자.

봉사기관리자는 하루동안에 봉사기를 회복할 충분한 능력이 있다고 가정하자. 또한 그는 년간 50,000딸라의 적당한 봉급을 받고 이 체계를 리용하는 30명의 프로그람수들의 봉급은 년간 60,000딸라라고 가정하자.

- 관리자의 봉사기회복시간 = 192딸라
- 자료의 하루의 가치를 회복하는 기술적시간 = 6,923딸라
- 봉사기가 차단된것으로 인한 기술적시간 = 6,923딸라
- 하루의 중지로 인한 전체 비용손실 = 14,038딸라

명백히 봉사기의 하루동안 멈춤으로 인한 비용은 여분의 디스크, RAID묶음, 지어 교대용봉사기의 사용비용을 쉽게 정당화할수 있다.이 계산에서는 관리성원들이 계획된 출하날자를 보장하지 못함으로 하여 초래되는 손실된 수입과 인기저하에 대하여서는 고려하지 않았다.

기관안의 자원에 대하여 시간척도를 규정하였다면 그와 관련한 인자들을 모두 고려해야 한다. 자원의 분실 또는 손실은 생산성에 크게 영향을 미친다.

인식자원

2000년 2월에 있은 봉사거부공격이후에 많은 회사들(Yahoo, Amazon, eBay, Buy.com 등을 포함하여)은 자기들의 주식가격이 떨어 졌다는것을 알게 되였다. 이 손실은 오래동안은 아니였지만 소비자들과 주식소유자들의 신용에 큰 타격을 주었다.

2000년 10월에 있은 Microsoft의 체계를 침입한 사건때에도 어떤 사람들은 귀중한 원천코드가 남모르게 교체되지 않았는가 걱정하였다. Microsoft는 피해를 부인했으나 명백한 침입사건은 회사뿐만아니라 그의 제품들의 신용도 떨어 뜨리기에 충분하였다.

주 의

공개적으로 활동하는 회사들에서 그 이름은 현실적인 자산으로 전환될수 있다. 비밀적으로 존재하는 회사나 정부기관들에서도 그 이름은 매우 중요하다.
많은 경우에 기관들은 실제자료의 완전성을 유지하는데보다는 신용과 능력에 대한 인식을 유지하도록 하는것을 더 중시하는데로 나가고 있다.

인식을 잘못 가지는데서 오는 피해는 보안산업(법집행기구들을 포함하여)에서 일하는 사람들에게서 중요한 문제로 된다.

그들은 보다 좋은 보호체계를 설계하거나 법적활동을 추구하는데서 자기 동료들의 정보와 경험에 많이 의존하는것이다.

해킹공격의 교묘한 기술적세부들을 자유롭게 교환할수 있도록 고무하려는 시도에서 기여하는 회사들에 대한 인식을 유지하면서 련방수사국(FBI)에서는 기반구조보호 및 콤퓨터침입보호기구(IPCIS)를 창설하였다. 이 기구는 해커기술들과 프로그람에 대한 닉명의 교환소로서의 역할을 놀고 있다.

주 의

봉사거부공격(DoS)은 체계가 망통신을 못하게 하는것이다. DoS공격은 목표체계에서 하나의 봉사가 동작할수 없게 하거나 또는 모든 망접속이 거부 당하게 할수도 있다.

무엇으로부터 망자원을 보호하려고 하는가

잠재적망공격은 망에 접근권한을 가지고 있는 임의의 원천으로부터 올수 있다. 이 원천들은 회사의 크기와 제공된 망접속형식 등에 따라 넓은 범위를 가진다.

위험분석을 통하여 모든 잠재적인 공격원천들을 식별하여야 한다. 그 원천들을 보면 다음과 같다.

- 내부체계
- 현장사무실위치로부터의 접근
- 광지역망련결을 통한 기업상대에게로의 접근

- 인터네트를 통한 접근
- 모뎀규약변환기를 통한 접근

누가 망을 파괴하려고 하는가

앞의 장에서 우리는 리론적으로 누가 망을 손상시킬수 있는가를 보았다. 이제부터 이 잠재적인 위협들을 알아 보자.

다음과 같은 잠재적위협들이 있다.

- 종업원
- 림시성원 또는 상담자
- 경쟁자
- 기관과는 근본적으로 다른 견해와 목적을 가진 사람
- 기관이나 종업원에 대하여 불신을 가지고 있는 사람
- 인기 있는 기관을 공격하여 악명을 떨치려는 사람

회사나 기관에 따라 이 사항에 첨가할수 있는 다른 잠재적위협들도 있을수 있다.

중요한것은 매개 위협이 성과적인 공격에 의하여 무엇을 얻으려는것인가, 이 공격이 잠재적공격자에게 가치가 있는것인가 하는것이다.

공격의 가능성은 어떠한가

기관의 자원들과 그것들을 공격하려는 사람들을 알게 되였으므로 이제는 잠재적공격위험의 수준을 평가할수 있다.

망이 고립된 망인가, 아니면 광지역망, 모뎀규약변환기, 인터네트를 통한 내부 VPN 등과 같은 입구점들을 가지고 있는 망인가?

이러한 모든 련결점들이 강한 인증과 어떤 형태의 방화벽장치를 리용하는가?

공격자가 망자원에 접근하기 위하여 이 접근점들을 써먹을 가치가 발견될수 있는가? 명백히 전형적인 공격자는 작은 건축회사보다는 은행을 공격하려고 할것이다.

망의 공격가치를 평가하는것은 매우 주관적이다. 같은 기관안의 두 사람이 공격의 가능성에 대하여 완전히 서로 다른 의견을 가질수 있다. 그러므로 기관안의 여러 부서들의 의견들을 고려하여야 한다. 또한 위험평가를 결정하는데서 경험 있는 상담자를 데려 올수도 있다. 공격의 가능성을 될수록 명백히 정의하고 리해하는것이 중요하다.

직접비용은 얼마인가

매개의 목록에 있는 자산에 대하여 그 자원이 손상되거나 파괴되였을 때의 직접비용을 기록한 다음 장기적효과는 포함시키지 말고 그저 망자원으로서 접근불가능하게 되였

을 때의 비용손실을 계산한다.

실례로 우리가 앞에서 본 하드구동기고장의 경우에 직접비용은 봉사기가 멎어 있는 매 분당 기술직원들의 잃어 진 생산성으로 정의되는데 약 14.5딸라이다.

직접비용을 정량적으로 취급하기 어려운 경우도 있다. 실례로 망손상으로 하여 경쟁자가 새로운 생산선의 도면이나 부분품목록 등에 접근할수 있게 되였다면 어떻게 될것인가? 이렇게 되면 경쟁자는 더 좋은 제품을 개발할수 있고 남의 제품을 시장에서 내쫓게 될것이다. 이러한 경우에 손실은 재난적인것으로 된다.

량적으로 계산하기는 보다 어렵지만 보다 실제적인것은 신용의 손실 또는 약점의 인식이다. 투자가들과 소비자들의 신뢰가 손상되는것은(종업원들의 사기가 떨어 지는것은 내놓고도) 보통 낮은 주식가격에 반영되며 이 모든것은 최종결과에 영향을 줄수 있는 직접적인 반응이다.

그러나 때로는 화폐비용이 손실을 결정하는데서 기본인자로 되지 않는 때도 있다. 실례로 공격자가 병원의 의학보고서들을 파괴한다면 이것은 생명에 대한 비극적인 손실을 초래할수 있다. 손실에 대한 직접비용을 계산할 때 딸라값만을 보아서는 안된다.

장기적회복비용은 얼마인가

손상으로부터 회복할 때의 비용을 계산하여 보자. 이것은 여러가지 준위의 손실로 인한 금융적충격을 리해하는것에 의하여 평가한다.

실례로 기업의 정보를 가지고 있는 봉사기가 주어 졌다고 하면

- 모든 리용자들을 차단하는 순간적인 고장을 회복하는데 소비되는 비용은 얼마인가?
- 일정한 시간동안 자원에 도달 못하게 하는 봉사거부공격으로 인한 비용은 얼마인가?
- 손상되거나 지워 진 중요한 파일을 회복하는 비용은 얼마인가?
- 하나의 장치부속품의 고장을 회복하는 비용은 얼마인가?
- 완전한 봉사기고장을 회복하는 비용은 얼마인가?
- 정보가 도난 당하고 도적을 잡지 못했을 때의 회복비용은 얼마인가?

여러 준위의 손상을 회복하는데 소모되는 비용과 손상이나 공격이 얼마나 자주 일어 나는가 하는것에 의하여 망의 재난복구에서의 금융적충격을 결정하는 척도를 얻을수 있다.

이와 같은 내용들에 기초하여 자원을 안전하게 하기 위해서는 마땅히 얼마나 소비해야 하겠는가를 알수 있을것이다. 어떤 자산(평판이나 소비자와 투자가의 신뢰 등)은 량적으로 취급하기 어려우나 그래도 현실적이라는것을 알아야 한다.

어떻게 망자원을 효과적으로 보호할수 있는가

망환경이 어떤 보호수준에서 얼마만한 비용의 보안이 필요할것인가를 고려하여야 한다.

실례로 원격접근이 없는 5명의 사용자구조로 된 회사에서 한사람의 일감으로 보안전문가를 채용하는것은 아마 지나친 일일것이다. 마찬가지로 은행이 보안방책에 대한 고려없이 외부망접근을 허용한다는것도 역시 생각할수 없는 일이다.

아마도 대부분은 우의 두 실례사이의 어떤 곳에 떨어 질것이므로 좀더 어려운 보안선택문제를 대상해 보자.

파케트려과가 인터네트접속을 보호하는데 충분한가? 아니면 방화벽에 투자해야 하는가? 하나의 방화벽이면 충분한가, 아니면 두개에 투자해야 할것인가? 이것들은 매일 보안전문가들에게 제기되는 결정문제의 일부이다.

일러두기

일반적인 지침은 특정의 자산을 보호하기 위한 모든 보안대책들의 비용은 재난으로부터 그 자산을 회복하는 비용보다 적어야 한다는것이다.
이것은 잠재적위협들과 함께 회복비용을 정량화하는것이 중요하다는 리유로 된다.
현대적인 망환경에서 보안예방조치가 필요하지만 많은 사람들은 이 예방조치에 소비되는 비용의 정당성을 증명할것을 요구한다.

비용을 증명하는것은 그리 어렵지 않을수 있다. 실례로 우리는 앞에서 봉사기의 하루정지가 14000딸라이상의 비용을 손실 본다는것을 보았다. 명백히 이것은 RAID묶음을 가지는 완전한 고성능의 봉사기에 투자하기에 충분한 비용증명으로 된다.

환경을 안전하게 하기 위한 비용들이 잠겨 져 있을수 있는데 이 비용들도 계산되여야 한다.

실례로 손상을 감시하기 위하여 모든 망활동을 기록해 두는것은 누군가가 시간을 들여 이 모든 기록들을 뒤져 보지 않는다면 필요가 없다. 이것은 환경의 크기에 따라 그자체로서 한 사람의 옹근일감이 될수도 있다. 망에 대하여 보다 세부적으로 기록하자면 새로운 보안일군이 필요하게 될수도 있다.

또한 보안이 강화되면 망자원을 리용 또는 접근하는데서 말단사용자에게 귀찮고 시간을 소비하는 일들이 생기게 된다. 이것은 이러한 리용의 복잡성을 피해야 한다는 것을 의미하지 않는다. 그것은 환경을 안전하게 하기 위하여 필요한 일일수 있으며 잃어 진 생산성에서의 잠재적인 비용으로 보아야 한다.

요약해 보면 보안조치를 위하여 자금을 요구하기에 앞서 이러한 조치들을 취하지 않았을 때의 상태를 설명하여야 한다. 또한 이러한 예방조치의 진짜비용이 무엇인가를 정확히 식별하여야 한다.

내가 관리자상급에 지배되는가

품을 들여 자기의 망의 정확한 위험분석을 하였다고 해도 최소수준의 보안요구를 지시하는 어떤 형태의 관리자상급기관이 있을수 있다. 이러한 정황에서는 간단히 보안대책들에 대한 비용증명만으로는 충분하지 않을수 있다. 회사의 비용지출에 관계없이 어떤 최소의 보안요구를 지시할수 있다.

실례로 어떤 군사적계약과 관련되여 회사는 많은 보안요구를 엄밀히 지켜야 한다. 대표적으로 결정된 보안조치는 유일하게 접수가능한 보안방법인것이 아니라 허용된 최소준위이다.

주 의

정부와 일할 때 많은 계약자들은 국가보안기관이 평가한 특정의 제품들을 쓰는 콤퓨터체계를 리용하도록 지시된다.

보안요구를 지시하는 정부적관리의 다른 실례로는 어린이개인비밀보호운동(COPPA)과 건강보험회사(HIPAA)를 들수 있다. 미국에는 아직 전자상업과 관련한 개인비밀관련법을 가지고 있지 못하지만 다른 나라들(주로 유럽나라들)은 회사들에 어떤 자료가 수집되고 보관될수 있는가를 엄격히 통제하고 있다. 만일 보안이 어떤 형태의 관리기관에 복종된다면 위험분석에서 비용증명부분은 변경되여야 할것이다.

보안실현을 위한 예산안 세우기

이제는 어느 수준의 보안에 대하여 거기에 소비되는 비용이 정당한가를 증명할수 있을것이다. 여기에는 가격이 눅어 질수 있는 항목들(봉사기하드웨어, 방화벽 등)과 재현되는 비용들(보안인원, 검사 및 체계관리)을 포함시켜야 한다.

《닭알을 모두 한바구니에 넣지 마시오.》라는 옛말을 상기하시오. 이 말을 보안예산을 세우는데 적용할수 있다. 예산을 한가지 보호방식에 다 소비하지 말아야 한다.

실례로 만일 어떤 사람이 쉽게 정문으로 들어 와 기업봉사기를 가지고 가버릴수 있다면 방화벽기술에 15000딸라를 투자하는것은 그리 좋은 일이 못된다.

일러두기

그러나 예산지출을 기관안의 다른 집단들과 결합하는것이 가능할수 있다. 실례로 망하드웨어와 봉사기에 대한 안전하고 통제되는 환경의 비용증명을 하기 어렵다면 그 망에 PBX, 음성우편, 전자설비 등을 다 넣고 비용증명을 할수 있을것이다.

또 한가지 실례는 이 장의 앞에서 본 기술봉사기문제이다. 기사들은 항상 추가적인 봉사기억공간을 요구한다. 봉사기기억을 새로 갱신할 때 여분의 디스크체계를 받아 들이고 기술부서에로 가는 비용의 일부를 청구할수 있을것이다.

보안예산을 세우는데서 어떤 회사들은 보안보험을 새롭게 추가한다. 얼핏 보면 별난

일 갈지만 대부분의 IT전문가들은 그 자료들의 가치와 이러한 예방조치의 필요성을 쉽게 리해할수 있다.

최종결과는 창조적이여야 한다. 보안예산을 더 늘여야 보다 많은 보안조치를 취할수 있다.

보안은 혁신적인 지출이라고 말할수 있다. 그 의미는 망이 피해를 본후에 더 많은 돈을 소비하지 않고 투자에 대한 결과를 실현할수 있다는 희망을 가지고 보안에 돈을 투자한다는데 있다. 보다 많은 예방조치를 취할수록 재난의 가능성은 더 적을것이다.

자료들을 문서로 만들기

이제는 자기의 모든 자산들을 알게 되였고 매일매일의 사업에서 그것들의 가치를 분석하였으며 매개의 회복비용을 평가하였다. 이제 시간을 좀 들여서 얻은 자료들을 형식화하고 문서로 만들자. 이 일이 필요한것이라는 리유는 많이 들수 있다.

우선 이러한 문서들을 가지고 있으면(전자적이든 하드복사든) 매개 보안대책에 대한 론증을 시작할 때 도움이 된다.

문서화된 수자들과 그림들을 가지고 론의하는것은 말로 론의하는것보다 훨씬 더 어렵다.

모든 자료들을 앞에 한줄로 세워 놓음으로써 후에 피해처리를 할 가능성이 더 적어 지게 될것이다.

이 문서는 후에 시간이 흐름에 따라 조절될것을 고려하여 류동적이여야 한다.

침입이나 고장의 비용을 평가할 때 100% 정확한것은 없다. 만일 정확도문제에서 운수가 나쁜 사람이라면 문서들을 개선하고 갱신할 기회들을 고려하여야 한다.

망환경도 시간에 따라 변화된다.

회사의 사장이 사무실에 들어 와서 《새로운 현장사무실을 하나 설치해야 하는데 어떤 설비가 필요하고 얼마만한 비용이 들겠는가?》라고 말한다면 어떤 일이 생길것인가? 현재의 비용들을 보여 주는 형식화된 문서를 가지고 있으면 쉽게 이 수자들을 뽑아 낼수 있다.

이 정보는 보안방책을 형식화할 때에도 매우 유용하다. 많은 사람들은 망보안의 중요성에 대하여 매우 불충분한 리해를 가지고 있다. 더우기 이것은 누가 예산의 돈주머니끈을 쥐고 있는가 하는 경영상의 문제들도 포함한다.

보안방책작성에서 침입이나 공격에 대하여 화폐값을 대치시키면 항목들을 증명하기가 한결 쉽게 된다.

실례로 회사의 사장은 자기 정보의 손실이 자기의 봉급과 맞먹는 비용손실을 준다는것을 깨닫기전에는 모든 내부자료를 암호화할 필요성을 알지 못할수도 있다.

보안방책을 세우기

대부분의 관리자들이 묻는 첫 질문은 《왜 형식화된 보안방책이 필요한가?》하는것이다. 보안방책은 많은 기능을 수행한다.

그것은 허용가능한 망활동과 잘못 사용하였을 때의 처벌내용을 상세히 서술한 기본문서이다.

보안방책은 또한 전체로서의 기관에 보안목표와 대상을 지적하고 명백히 하기 위한 연단을 제공한다.

좋은 보안방책은 매개 종업원에게 안전한 환경을 유지하는데 어떤 책임이 있는가를 보여 준다.

주 의

보안방책의 한 실례로 부록 2를 보시오.

보안방책의 기초

보안방책은 흔히 문제가 제기되여야 관심하게 된다.

개별적인 문제에 집중하는것이 매개 점을 식별하는 가장 쉬운 방법이다. 어떤 환경에서는 간단히 《사업과 관계 없는 인터네트사용은 나쁘다.》라고 말하는것이 허용되지만 이 방책을 따라야 하는 사람들은 《사업과 관계 없는 사용》과 《나쁘다》라는 말이 실제로 무엇을 의미하는지 알 필요가 있다.

보안방책이 집행되려면 다음과 같은것이 필요하다.

- 기업의 다른 방책들과 일치하는것
- 망지원부서와 적당한 관리수준에 허용되는것
- 현존망설비와 프로그람들을 리용하여 집행가능한것
- 지역 및 국가, 련방법들에 맞는것

일치성이 열쇠이다

일치성은 사용자들이 그 방책을 불합리한것으로 보지 않도록 담보한다. 보안방책의 전체적인 주제는 보안에 대한 기관의 견해를 반영하여야 하며 일반적으로 접수할수 있는 기업의 실천이여야 한다. 만일 회사가 물리적보안 또는 회사자산의 리용에 대하여 매우 완만한 태도를 가지고 있다면 엄격한 망리용방책을 집행하는것은 어렵거나 무의미할수 있다.

실례로 어떤 회사의 소유자는 망에 대한 모든 원격접속은 가능한 가장 긴 암호열쇠를 리용하여 암호화되여야 한다고 주장하였다. 원격사용자들은 서로 다른 가입이름과 통과암호를 가져야 하고 이 구좌들에는 최소접근량만이 제공되였다. 또한 특수한 필요성을 증명하지 않는한 원격접속은 금지되였다.

이것은 그다지 억지공사 같지는 않지만 이 망이 들어 있는 시설은 세자리코드를 가

지는 하나의 암호자물쇠만에 의하여 보호되였다. 그 시설은 경보체계를 가지고 있지 않았고 도난 당해도 모를 위치에 있었다. 암호열쇠를 위한 문자조합은 7년이상이나 변경되지 않았다. 또한 종업원들은 이 문자조합을 필요하다고 하는 아무에게나 주군 하였다.

이것까지도 그리 나쁘지 않았지만 내부구좌에 대해서는 통과암호요구조차 없었다. 많은 사용자들(소유자도 포함하여)이 자기의 구좌에 배당된 통과암호를 가지고 있지 않았다. 두개의 봉사기가 있었는데 쉽게 접근할수 있는 위치에 있었다.

이 회사는 원격접근보안에 관해서는 아마 정당하였을수 있으나 취해 진 대책들은 회사의 다른 보안방책과 비교할 때에는 모순되는것이였다. 원격접근보다 더 높은 우선권을 가져야 하는 다른 문제들도 있었다. 이 소유자는 원격접근방책이 회사의 다른 보안문제들과 일치하지 않기때문에 그것을 집행하기 어렵다고 생각했던 모양이였다. 종업원들이 그 시설에 대한 물리적접근은 중요시하지 않는다는것을 알고 있는데 인터네트접속이 왜 달라야 하겠는가?

기관안에서의 허용

보안방책이 집행되자면 기관안에서의 일정한 권위자들이 접수할수 있어야 한다. 만일 경영자측이 방책이 제공하는 리익을 알지 못하고 인정하지 않는다면 그 보안방책을 집행하는것은 실패할수 있다.

경영자측의 허가가 없을 때 무슨 일이 발생할것인가에 대한 한가지 좋은 실례는 란달 슈와르쯔(Perl프로그람언어의 기본창시자)와 인텔회사간의 법적소송사건이다. 그는 인텔회사를 위하여 개인청부로 일하고 있었는데 인텔의 보안방책에 따라 보지 말아야 할 정보에 접근한것으로 하여 고소되였다.

인텔은 이 사건에서 이겼지만 이 법적사건은 슈와르쯔에게 유죄판결을 내리는데 리용하려던 보안방책이 인텔의 정식종업원들에게도 적용되지 않았다는것이 밝혀짐으로써 크게 약화되였다. 재판에서 증명되였지만 인텔의 부리사장이며 총지배인은 인텔의 보안방책을 따르지 않아도 되도록 허가되였던것이다.

사건을 더 애매하게 한것은 그가 그 방책에 따르지 않고 오유를 범한데 대하여 인텔이 그를 문책하지 않은것이다.

이것은 인텔의 보안방책이 류동적이며 슈와르쯔는 죄없이 선택되였다는 인상을 남겼다.

기관의 보안방책은 경영자측의 모든 준위에서 접수되고 집행되여야 한다. 성과적으로 집행되려면 이 방책은 모든 망사용자들에게 동일하게 적용되여야 한다.

집행가능성

보안방책이 좋은 방책이 되려면 집행가능하여야 한다. 《매개 망사용자는 자기의 통과암호를 90일에 한번씩 바꾸어야 한다.》라고 하는것은 망조작체계가 기간완료되지 않고 이 90일한계를 초과한 구좌를 차단한다면 효과가 적을것이다.

집행될수 없는 방책들을 법적으로 만들수는 있지만 실천적으로 그렇게 하는것은 현명한 선택이 못된다. 사용자들이 기업의 방책을 무시해도 확인이 없으므로 일 없다는 인상을 가지는것을 원하지 않을것이다. 만일 확인이 없다면 불복종에 대한 후과도 없다.

일러두기

> 하나의 망리용방책에 불복종하는것은 빨리 도미노효과를 일으켜 모든 망리용방책들을 무시하게 할수 있다. 처음으로 망리용방책을 세울 때에는 그 리용을 100% 확인할 필요가 없으나 방책을 집행하는것이 문제거리가 되지는 않는가 하는것을 어떤 방법으로 감시 또는 보고되게 하여야 한다.

때로는 특정한 방책의 모든 측면을 적극적으로 감시하는것도 충분하지 못할 때가 있다. 적당한 방법으로 이러한 론쟁점들을 퍼뜨릴수 있다. 실례로 보안방책은 보통 회사고유인것으로 고찰된다.

그러나 회사의 밖에 있는 사람들에게 영향을 미치는 방책항목이 있을수 있다. 이 항목들은 그것들이 집행가능한것으로 되도록 담보하기 위하여서는 공개되여야 한다.

인터네트상에서 돌아 가는 한가지 이야기가 있는데(그것은 사실일수도 있고 아닐수도 있다.) 그것은 한 회사가 자기의 체계를 파괴한 원격공격자를 어떻게 감시, 추적하여 찾아 냈는가를 서술하고 있다.

이야기에서는 경찰이 혐의자를 체포하여 기소된 자가 법정에 나서게 되였다. 재판에서 기소된 자는 문제의 망자원에 접근하였음을 인정하였다. 그의 진술에 의하면 그는 자기가 나쁜 짓을 하고 있다는 생각을 하지 않았다는것이다.

왜냐하면 그 자원에 접근하자 곧 《환영합니다.》(Welcome)라는 화면이 나타났기때문이였다.

변호에서는 그가 이 자원에 접근하지 말아야 한다는것을 결정하는것이 그의 능력밖의것이라는것이 주장되였다. 또한 피고인의 변호사는 땅소유자가 다른 사람이 그 땅에 들어 오지 않도록 공시를 내보일것을 요구하는 지방법을 상기해 내였다.

재판관은 고급한 콤퓨터범죄보다는 지방법에 관련시키는것이 더 쉽다고 보고 변호측의 주장을 받아 들여 혐의자를 석방하였다.

망보안방책은 적당히 공개되여야 한다. 이 방책들을 서술하는데서 가입규약과 말단통보문과 같은 명백한것들을 놓치지 말아야 한다.

지역 및 국가법, 련방법과의 일치

보안방책들을 실현하기에 앞서 법전문가들의 검열을 받아야 한다. 어떤 방책항목의 부분이 비법적이라고 판단되면 그 항목(또는 그 방책자체)은 페기될수 있다.

실례로 《위반하는 사람은 태형에 처한다.》는 방책은 태형이 비법화되여 있으므로 법에 의하여 금지될것이다. 침해 당한 사람은 망을 손상시킨 공격자를 때려 주고 싶겠지만 이러한 불법적인 앙갚음으로 하여 그는 상환청구의 모든 기회를 버리는것으로 될수 있다.

이에 대하여서는 정당하게 표현하는것이 중요하다. 모든 방책들을 세심하고 정확하게 법적술어로 쓰는것이 좋다.

법적인 검토는 매 방책항목들의 효과를 리해하는데서 도움이 된다. 상세한 표현을 쓰지 않으면 좋은 의도의 방책도 부정적인 효과를 가져 올수 있다.

최근의 한 법정사건에서 한 종업원이 작업중에 색정싸이트를 우연히 본것으로 하여

17만 5000딸라를 번 일이 있었다. 어떻게 그는 자기의 고용주가 책임을 지도록 하였는가? 그 수상한 싸이트가 회사소유의 Web봉사기에 위치하고 있었는가?

그 대답은 독자들을 놀라게 할것이다. 회사는 《색정싸이트들은 차단되며 회사의 망에 접근될수 없다.》라는 기업방책을 가지고 있었다. 회사는 수상하다고 인정되는 싸이트들에로의 접근을 려과하고 있었다. 그런데 인터네트상에 《수상한》 싸이트들이 너무 많아서 그것들을 모두 막을 방도가 없었다.

법정에서는 회사가 이른바 수상한 싸이트들을 모두 차단함으로써 계약을 끝까지 유지하지 않았기때문에 계약자의 위반에 대하여 책임져야 한다고 판결하였다.

이 싸이트들을 려과한다는 방책을 제정함으로써 회사는 《이 활동의 성과적수행을 위한 책임을 접수》하고 있었으며 이로 하여 책임을 지게 되였다.

그 종업원의 《고용》에 대한 배상금은 이러한 《발견》에 기초하고 있었다.

이 방책항목은 어떻게 썼어야 하였는가? 다음의 서술을 고찰하여 보자.

《종업원의 직업상 책임을 수행하는것과 다른 목적으로 회사소유의 자산을 가지고 인터네트싸이트에 접근하는것은 해고의 리유로 간주된다. 회사는 이에 대한 순응을 담보하기 위하여 모든 종업원들의 망활동을 감시하고 려과할 권리를 가지고 있다.》

이 서술은 불필요한 싸이트들을 금지함으로써 같은 방책을 실행한다. 여기서는 여러가지로 해석될수 있는 《수상한》이라는 단어를 없애 버렸으며 종업원의 직업과 관계 없는 모든 Web싸이트접근을 금지하고 있다. 또한 복종의 책임을 고용주가 아니라 종업원에게 지우고 있으며 회사에는 이 싸이트들을 려과하는것을 허용하고 있다.

일러두기

적당한 표현은 세계안의 모든 차이를 좋은 보안방책과 나쁜 보안방책사이에 있게 할수 있다.

훌륭한 보안방책을 세우려면 무엇이 필요한가

좋은 보안리용방책은 최소한 다음과 같아야 한다.

- 기관의 모든 성원들에게 쉽게 접수될수 있어야 한다.
- 보안목적들은 명백히 모임을 정의하여야 한다.
- 방책에서 론의된 매 항목을 정확히 정의하여야 한다.
- 매 항목에서 기관의 위치를 명백히 보여 주어야 한다.
- 매 항목을 고려하는 방책의 정당성을 증명하게끔 서술하여야 한다.
- 서술된 항목과 관련하여 종업원들의 역할과 책임을 서술하여야 한다.
- 서술된 방책에 복종하지 않았을 때의 결과를 써야 한다.
- 서술된 항목과 관련하여 세부 또는 명백성을 위한 접촉정보를 제공하여야 한다.
- 사용자가 바라는 개인비밀수준을 정의하여야 한다.
- 특별히 정의되지 않은 문제들에 대한 기관의 립장을 포함시켜야 한다.

접근가능성

보안방책을 대중적인것으로 되게 하는것은 그 효과성에서 기본으로 된다. 앞에서 언급하였지만 가입등록과 말단통보문이 좋은 시작으로 된다.

만일 종업원수첩을 가지고 있다면 보안방책을 이 문서와 결합시키는것을 생각할수 있다.

또한 기관이 자기의 인트라네트Web싸이트를 가지고 있다면 이 문서들을 그 싸이트에 첨가할수 있다.

보안목적들을 정의하기

간단한것 같지만 기관에서 보안이 왜 중요한가를 정의하는 목적을 명백히 서술하는것은 매우 유익하다.

목적을 잘 서술하여야 방책항목들이 하찮거나 불필요하다고 생각하지 않을수 있다.

표준이나 지침들을 제정할 때에는 그것이 제공하는 유리한 점을 사람들이 리해하도록 하여야 한다.

일러두기

부록 2에 보안방책의 한 실례가 있다. 독자들이 보안방책을 만들 때 이것을 안내서로 리용할수 있다.

매 항목을 정의하기

매 방책항목을 서술할 때 최대한 명백하고 정확하여야 한다. 모든 표현과 술어들이 될수록 정확하여야 한다.

실례로 일반적인 인터네트접근에 의존하지 말고 그 항목을 처리하는 특정의 봉사(전자우편, 파일전송 등)들을 알아야 한다.

만일 방책항목이 후에 집행되여야 한다면 그 방책을 정의하는것을 뒤로 미루는것이 좋다. 또한 자주 반복되는 일반적인 서술은 여러가지로 해석될수 있다.

일러두기

회사가 인터네트상에서 VPN기술을 리용한다면 정확한 서술이 보다 중요하게 된다. 인터네트상의 공개호스트와 VPN접속의 다른 끝에 위치한 호스트사이의 차이를 정확히 정의하여야 한다.

기관의 위치

방책항목에 대한 기관의 견해를 표현할 때 명백하고 간결한 술어를 써야 한다. 실례로 《접수할수 없는》과 같은 형용사는 많은 모호한 점들을 가지고 있다.

어떤 종업원의 행동이 《접수할수 없는》것일수 있지만 반드시 어떤 방책에 대한 위반으로 되는것은 아니다.

방책을 서술할 때 명백하고 간결한 의미를 가지는 단어들을 골라 써야 한다.

부정적인 실례로서 《위반》, 《계약어김》, 《범죄》, 《악용》등을 들수 있다. 긍

정적인 실례로는 《허용할수 있는》, 《합법적인》, 《허가된》, 《권한을 가진》등 이다. 모호한 술어들을 피함으로써 방책의 의미와 불복종의 결과가 명백해 지고 집행가능하다는것을 확신할수 있다.

방책의 정당성을 증명하기

이것은 망사용자들에게 방책의 매 점이 왜 중요한가를 보여 주는것이다. 실례로 《전자우편은 보안되지 않는 매체로 간주되므로 회사의 내부정보를 다루는데 그것을 리용하는것은 허용되지 않는다.》라는 서술은 방책항목과 그 증명을 동시에 말하는것으로 된다.

그 항목이 언제 적용되는가?

어떤 환경에서 그 방책이 유효한것으로 적용되는가를 명백히 하여야 한다. 그 방책이 모든 사용자들에게 동일하게 영향을 주는가, 아니면 어떤 일정한 성원들에게만 영향을 미치는가, 근무시간이후에도 유효한가, 기본 사무실에만 영향을 주는가, 아니면 현장사무실에도 적용되는가?

방책이 어떻게 적용되는가를 명백히 설정할 때 그것이 가져 올수 있는 충격도 명백히 하여야 한다.

이것은 이 방책이 누구에게 적용되는가에 대한 불확실성이 없다는것을 담보한다. 어떤 종업원이 그 방책을 자기를 제외한 모두에게 적용되여야 한다고 가정할수 없게 하여야 한다.

역할과 책임

사슬은 그것의 가장 약한 고리만큼만 강하다. 그러므로 모든 성원들이 보안에 대하여 책임이 있다는것을 명백히 하여야 한다.

보안은 어떤 특정한 사람만이 수행하여야 할 일감의 한부분인것이 아니라 전체의 관심사이다.

누가 보안방책을 집행하는데 책임이 있으며 이 사람에게 기관으로부터 어떤 권한이 부여되였는가를 명백히 하여야 한다.

불복종의 결과

한 종업원이 어떤 보안방책항목을 지키는데서 실수를 하였거나 또는 무시해 버렸다면 어떻게 될것인가? 기관은 이에 곧 반응하여 대책을 취해야 한다.

방책에는 불복종에 대한 가능한 처벌내용이 서술되여 있어야 한다.

이 서술은 법적이고 명백히 정의하는것이 중요하다. 《적당한 조치가 취해 질것이다.》라고 하는것은 미칠수 있는 영향의 엄중성을 서술하지 못한다.

방책을 서술하는 사람들이 적당한 처벌내용을 찾을수 없다면 많은 경우 처벌은 효과적인것으로 되지 못한다. 그러나 처벌의 엄중성은 기관이 그 항목을 얼마나 중요하게 보는가를 표현하므로 적당한 처벌을 배당하는것이 매우 중요하다.

실례로 쓸데 없이 전자우편을 보내는것은 문책의 기초로 간주될수 있으며 가정용콤

퓨터의 가장 좋은 가격을 찾기 위하여 Web를 돌아 다니는것은 말로 하는 경고만을 받을뿐이다.

불복종의 결과를 서술할 때 기관이 어떤 행동을 취할것인가를 구체화하여야 한다.

보다 많은 정보를 위하여

어떤 특정항목의 있을수 있는 모든 측면들을 명백히 정의하는 방책을 형식화하는것은 어렵다. 그러므로 보충적인 정보들을 제공하는데 책임 있는 자원을 확인하여야 한다.

개인의 책임은 변할수 있으므로 이 자원을 이름으로가 아니라 직업기능으로 확인하여야 한다.

《모든 질문은 XX에게 발송하라.》라고 쓰는것보다는 《보다 많은 정보를 얻으려면 관리인과 상담하시오.》 또는 《이 문제와 관련한 모든 질문은 망보안관리자에게 직접하시오.》라고 쓰는것이 더 좋다.

개인비밀보호의 수준

개인비밀보호문제는 항상 중요한 문제로 제기된다.

기관의 자원으로 보관된 정보에 관하여 개인비밀에 대한 관점을 명백히 서술하여야한다.

만일 회사가 보관된 정보의 모든 소유권을 명백히 주장하지 않는다면 이 정보는 종업원의 재산으로 해석될수 있다.

회사의 내부정보는 비밀이라고 가정하지 말아야 한다. 여러해전에 널리 공개된 한 사건을 실례로 보자. 한 고급경영자가 자기직업을 버리고 기본경쟁자에게로 넘어갔었다.

이 사람이 비밀정보들을 가지고 간것으로 의심하여 회사는 그의 모든 전자우편통보문들을 모아서 검열하여 보았다. 그들은 회사가 자기의 경영우세를 유지하는데서 사활적이라고 보는 정보들을 그가 가져 갔다는 증거를 발견하였다.

그러나 이 사건을 법정으로 가져 갔을 때 전자우편은 증거로 간주될수 없게 되였다.

그것은 전자우편을 회사소유의 자원으로 보는 명백한 방책이 없었기때문이였다.

피고측은 전자우편은 일반우편과 같은것이고 개인비밀의 같은 수준을 가지고 있다고 주장하였다.

재판관은 법정의 승인없이 개인의 우편함를 열수 없다는것을 잘 알고 있었다.

피고측은 이런 정황에서 회사는 우편국과 같은 방책을 지켜야 한다고 주장하였다. 결국 전자우편은 증거로 될수 없다고 선포되였으며 회사는 증거가 없는것으로 하여 사건에서 패하고 말았다.

이 이야기의 교훈은 망자원의 소유권을 주장하는것 그리고 서술된 보안방책을 집행하기 위하여 취할수 있는 대책들을 써놓는것이 매우 중요하다는것이다.

특별히 정의되지 않은 항목들

방화벽을 실현할 때 망통신량과 관련하여 두가지의 립장이 있을수 있다.

첫째는 《명백히 허용되지 않는것은 거부한다.》이고 두번째는 《명백히 거부되지

않는것은 허용한다.》이다. 첫째것은 보안과 관련하여 엄격한 립장이고 둘째것은 보다 관대한 립장이다.

이 같은 원리들을 망에 적용한다. 명백히 정의되지 않은 문제들에 대하여 엄격한 또는 열린방책을 설계할수 있다.

이것은 보안방책에서 특별히 정의되지 않은 항목이 제기될 때 후퇴할 자리를 제공한다. 분명 어떤것은 잊고 언급하지 못할수 있으므로 이것은 좋은 생각이라고 볼수 있다.

보안방책에서 표면적으로 취급되지 않은 항목들에 대한 기관의 립장을 보여 주는 서술이 있어야 한다. 어느 방법이 보다 적당한가는 만들려고 하는 보안방책이 얼마나 엄격한가에 달려 있다. 그러나 대표적으로 보안에 대하여 엄격한 자세로 시작하고 필요가 제기될 때 추가적인 방책들을 보충하는것이 보다 쉽다.

좋은 보안방책의 실례

좋은 보안방책의 개별적인 점들을 다 보았으므로 이제는 이 점들을 어떻게 묶겠는가를 보여 주는 구체적인 실례를 고찰하자. 부록 2에는 더 많은 실례들이 있다.

다음의것은 방책서술초록의 한 실례이다.

인터네트Web봉사기자원에로의 접근은 직업관련과제수행의 명백한 목적에 대하여서만 허용된다.

이 방책은 망자원의 효과적인 리용을 담보하기 위한것이며 모든 종업원에게 동등하게 적용된다. 이 방책은 생산 및 비생산기간동안에 집행된다.

모든 Web봉사기접근은 망담당자에 의하여 감시될수 있으며 종업원들은 자기의 직속상급에게 Web봉사기접근의 리유를 밝혀야 한다. 이 방책에 응하지 않으면 서면으로 경고문이 배포될것이다. 인터네트자원의 Web봉사기접근허가와 관련한 보충적인 정보를 위해서는 자기의 직속상급과 상담하시오.

이제 이 서술이 우리가 론의하는것을 다 포함하고 있는가를 보기로 하자.

매개 항목의 정의 이 방책은 인터네트Web봉사기자원에 대한 접근을 취급한다. 이 서술은 그것이 속하는 항목을 정확히 정의한다.

기관의 위치 이 서술은 인터네트접근이 《직업관련과제수행을 위한 명백한 목적을 위해서만 허용된다.》고 선언하고 있다. 기관의 립장은 명백하다. Web검색은 직업관련활동을 수행하기 위해서만 허용된다.

방책의 증명 인터네트접근의 제한을 증명하기 위하여 방책에서는 《이 방책은 망자원의 효과적인 리용을 담보하기 위한것이다.》라고 서술하고 있다. 이 표현은 명백하고 적당하다. 기관은 직업관련사업만으로 인터네트리용을 제한함으로써 인터네트통신량을 최소화하려고 하고 있다.

이 항목이 언제 적용되는가? 이 방책은 인터네트접근제한이 《모든 종업원에게 동일하게 적용되며 생산 및 비생산기간에도 집행된다.》고 규정하고 있다. 이것은 이 방책이 모든 시간 유효하며 모든 종업원들이 그 지침에 복종해야 한다는것을 밝히고 있다.

역할과 책임 이 방책은 망담당자가 적당한 Web봉사기접근을 감시할 책임을 지고 있다는것을 서술하고 있으며 《종업원들은 자기의 직속상급에게 Web봉사기접근의 리유를 밝히도록 하여야 한다.》는것을 보충하고 있다. 이것은 매 종업원들에게 인터네트Web봉사기접근을 증명할것을 요구한다. 그것은 또한 상관들이 이 증명을 인정한데 대한 책임이 있다는것을 보여준다. 또한 하급이 인터네트Web봉사기로 접근할 때 자기의 상급에게 알려야 한다는것을 가정한다.

불복종의 결과 이 방책은 다음과 같이 규정하고 있다. 《이 방책에 응하지 않으면 서면으로 경고문이 발송될것이다.》라는 짧고 친절하면서도 적당한 이 문장은 만일 종업원이 보안방책을 위반한다면 무슨 일이 생길것인가를 보여 준다.

보다 상세한것을 위한 접촉정보 마지막으로 이 방책은 다음과 같이 지적하고 있다.

《무엇이 적당한 인터네트자원의 Web봉사기접근으로 간주되는가에 대한 보다 많은 정보를 얻기 위하여서는 자기의 직속상급과 상담하시오.》라는 이 방책은 어떤 정보가 준비되여 있고 어디서 그것을 얻을수 있는가를 알리고 있다(이 방책은 여기서 상관의 대답 또는 어디서 그것을 얻을것인가를 알고 있다고 가정한다.).

개인비밀의 수준 개인비밀문제는 이 실례에서 간단히 언급되지만 직선적으로 지적하고 있다. 《Web봉사기접근은 망담당자에 의하여 감시될수 있다.》 이것은 사용자가 인터네트Web봉사기로 접근할 때 개인비밀보호를 기대할수 없다는것을 암시한다.

그러나 이 서술은 감시의 수준을 정의하지 않고 있다. 실례로 그것은 망담당자가 봉사기들, URL들 또는 실제적인 페지내용을 검열할것인가를 규정하지 않고 있다. 이 경우에 구체성이 부족한것은 결함으로 보지 말아야 한다.

왜냐하면 그것은 망관리자에게 조사의 수준에서 일정한 유연성을 허락하기때문이다.

요 약

이제는 자기의 환경이 요구하는 보안수준을 어떻게 평가할것인가에 대한 확고한 리해를 가져야 한다. 또한 어느 자원을 보호해야 하며 기관안에서 그것들의 고유한 가치는 어떠한가를 알아야 한다. 이 위험분석은 이 책에서 론의되는 매개 보안조치에 대하여 기초로 된다.

또한 효과적인 보안방책을 어떻게 서술할것인가를 알게 되였다.

다음장에서는 체계가 어떻게 통신하는가를 보기로 한다. 많은 보안침해자들은 통신규칙들을 악용하므로 망정보가 어떻게 교환되는가를 리해하는것은 이러한 공격에 대처하는데서 사활적인 문제로 된다.

제3장. 망체계통신에 대한 리해

이 장에서는 망에 련결된 체계들사이의 통신을 고찰한다. 여기서는 독자가 망주소배당과 같은 망의 기초를 이미 리해하고 있다고 가정한다. 이 장에서는 망케블을 따라 무엇이 진행되고 있는가 하는데 기본을 두고 고찰한다. 이 지식은 다음의 장들에서 보게 될 보안개념들을 리해하는데서 결정적인것으로 된다.

자료프레임의 해부

자료가 망을 따라 이동할 때 그것은 프레임이라고 하는 배포봉투안에 포장된다. 프레임은 망의 위상구조에 따라 다르다. 이써네트프레임은 통표고리형이나 AT 프레임과는 다른 정보를 가지고 있다. 이써네트는 현재까지 가장 널리 쓰이는 위상구조이므로 여기서는 그것을 상세히 보기로 한다.

이써네트프레임

이써네트프레임은 정보를 나르기 위하여 전송매체우로 전송되는 수자식임풀스들의 모임이다. 하나의 이써네트프레임은 64−1518byte만한 크기를 가지며 다음의 4가지 부분으로 구성된다.

- 준비신호(Preamble)
- 머리부(Header)
- 자료(Data)
- 프레임검사렬(FCS)

준비신호 준비신호는 모든 수신국들에게 《준비하라, 전송하겠다》라고 알리는 통신임풀스들의 렬이다. 표준적으로 준비신호는 8byte길이를 가진다.

주 의

준비신호는 통신과정의 부분으로 간주되고 전송되는 실제적인 정보의 부분은 아니므로 보통 프레임의 크기에는 포함되지 않는다.

머리부 머리부는 항상 누가 그 프레임을 보냈으며 어디로 가고 있는가에 대한 정보를 포함한다. 또한 프레임의 크기가 몇바이트인가 하는 정보도 포함하는데 이것을 길이마당이라고 하며 오유수정에 리용된다. 수신국이 길이마당에 지적된것과 크기가 다른 프레임을 받았다면 송신체계에 새로운 프레임을 보낼것을 요구한다. 길이마당이 리용되지 않는다면 머리부는 그 대신에 어떤 형식의 이써네트프레임인가를 설명하는 형식마당을 포함한다.

주 의

머리부의 크기는 항상 14byte이다.

자료 프레임의 자료부는 그 국이 전송하려는 실제적인 자료와 원천 및 목적지주소와 같은 통신규약정보가 포함된다. 이 자료마당은 46−1500byte크기이다. 만일 국이 1500byte보다 큰 정보를 가지고 있다면 전송을 위하여 그 정보를 여러개의 프레임으로 분할하고 순서번호를 리용하여 적당한 순서를 정한다. 순서번호는 목적지체계가 그 자료를 재조립하는 순서를 준다. 이 순서정보도 프레임의 자료부에 보관된다. 프레임이 46byte만한 정보를 가지고 있지 못하다면 뒤에 1을 채워 넣는다. 프레임형식에 따라 이 부분은 체계가 어떤 통신규약 또는 통신방법을 리용하고 있는가에 대한 추가적인 정보를 포함할수 있다.

프레임검사렬(FCS) 프레임검사렬은 수신된 자료가 실제로 전송된 자료라는것을 담보하는데 리용된다. 전송체계는 순환여유검사 또는 CRC라고 하는 알고리듬을 통하여 그 프레임의 FCS부분을 처리한다. 이 CRC는 우의 마당의 값을 취하여 4byte수를 만든다. 목적지체계가 그 프레임을 수신할 때 같은 CRC로 계산하고 그것이 이 마당안의 값과 같은가를 비교한다. 목적지체계가 불일치를 발견하면 전송과정에 그 프레임에 오유가 생겼다고 인정하고 그 프레임을 다시 보낼것을 송신체계에 요구한다.

주 의

FCS의 크기는 항상 4byte이다.

프레임머리부

이써네트프레임의 머리부에 대하여 더 상세히 고찰하자. 머리부정보는 누가 그 정보를 보냈고 어디로 보내는가를 식별하는데서 매우 중요한 책임을 지고 있다.

머리부는 전송의 원천지와 목적지를 식별하기 위한 두개의 마당을 가지고 있다. 이것들은 원천체계와 목적체계의 마디점주소들이다. 이 수값을 매체접근조종(MAC)주소라고도 부른다. 마디점주소는 망장치들(망기판 또는 망하드웨어)을 식별하는데 리용되는 유일한 주소이며 세계적으로 그것을 다른 망장치와 구별하는 유일한 식별자이다.

두 망장치는 결코 같은 번호로 지정될수 없다. 이것을 전화번호와 같이 생각할수 있다. 전화를 가진 매집에는 유일한 전화번호가 있어서 어느 번호를 호출하면 누가 나온다는것을 아는것과 마찬가지로 목적지체계의 MAC주소를 리용하여 프레임을 보내게 된다.

주 의

MAC주소는 애플회사의 콤퓨터와 관련해서는 아무 의미도 가지지 않으며 모두 대문자로 표시한다.

이 6byte, 12자리 16진수는 두 부분으로 나누어 볼수 있다. 주소의 첫 절반부분은 제작자의 식별자이다. 제작자에게 MAC주소의 한 부분이 배당되여 자기의 제품들을 식별하는데 리용한다. 중요한 몇가지 MAC주소의 부분을 표 3-1에 보여 준다.

표 3-1 MAC주소들

MAC주소의 첫 3byte	제작자
00000C	Cisco
0000A2	Bay Networks
0080D3	Shiva
00AA00	Intel
02608C	3Com
080009	Hewlett-Packard
080020	Sun
08005A	IBM

일러두기

MAC주소의 첫 3byte는 좋은 고장수리도구로 될수 있다. 만일 한 문제를 조사하고 있다면 그 원천 MAC주소를 결정하여 보시오. 누가 그 장치를 만들었는가를 알면 어느 체계가 고장나고 있는가를 쉽게 알수 있다. 실례로 첫 3byte가 0000A2이라면 망에서 Bay Networks의 제품들에 주의를 돌리면 될것이다.

MAC주소의 두번째 부분은 제작자가 그 장치에 배당한 계렬번호이다.

주목되는 한가지 주소는 FF-FF-FF-FF-FF-FF이다. 이것을 방송주소라고 한다. 방송주소는 특수한데 그것은 이 파케트를 수신하는 모든 체계가 그 자료를 읽어야 한다는것을 의미한다. 만일 한 체계가 방송주소로 보내지는 한 프레임을 만나면 그 프레임을 읽고 그 자료를 처리하게 된다.

주 의

원천마디마당에서 방송주소를 가지는 프레임은 있을수 없다. 이써네트에서는 원천마디마당에 방송주소가 놓이는 상태가 존재하지 않는다.

주소변환규약

목적지마디점주소가 무엇인가를 어떻게 알고 거기로 자료를 보낼것인가? 그런데 망기판은 전화번호책을 가지고 있지 않다. 마디점주소를 구하는것은 주소변환규약(ARP)프레임이라고 하는 특수한 프레임에 의하여 수행된다. ARP는 어느 통신규약(IPX, IP, NetBEUI 등)을 리용하는가에 따라 다르게 동작한다.

실례로 그림 3-1을 보시오. 이것은 같은 망에 있는 다른 체계에 정보를 보내려 하는 체계의 초기파케트를 해신한것이다. 전송체계는 목적체계의 IP주소를 알고 있지만 목적지의 마디점주소는 모르고 있다. 이 주소가 없으면 자료의 국부적전송은 불가능하다. ARP는 체계가 목적지체계의 마디점주소를 구하는데 리용된다.

그림 3-1. 목적지체계의 마디점주소를 얻으려는 전송체계

주 의

프레임해신은 2진프레임전송을 사람이 리해할수 있는 형식으로 변환하는 과정이다. 이것은 보통 망분석프로그람을 리용하여 수행된다.

ARP는 다만 국부적통신을 위한것이다. 자료파케트가 경로기를 지나갈 때 이써네트머리부는 다시 작성되는데 원천마디점주소는 경로기의것이고 전송체계의것은 아니다. 이것은 새로운 ARP요청이 생성되여야 한다는것을 의미한다.

그림 3-2는 이것이 어떻게 진행되는가를 보여 준다. 전송체계 F는 어떤 정보를 목적지체계 W에 보내려고 하고 있다. W는 F와 같은 부분망에 있지 않으므로 그는 국부경로기에 포구 A의 마디점주소를 알기 위하여 하나의 ARP를 전송한다. F가 이 주소를 알면 그는 자기의 자료를 경로기에 전송한다.

이때 경로기는 다음에 W의 마디점주소를 알기 위하여 포구 B에 하나의 ARP를 보낼것이다. W가 이 ARP요구에 응답하면 경로기는 그 자료로부터 이써네트프레임을 떼내고 새것을 만든다. 경로기는 원천마디점주소(원래 F의 마디점주소)를 포구 B의 마디점주소로 바꾼다. 또한 목적지주소(원래 포구 A)를 W의 마디점주소와 바꾼다.

주 의

경로기가 두 부분망과 통신하기 위하여서는 매 포구에 대하여 하나씩 두개의 유일한 마디점주소가 필요하다. F가 W를 공격하고 있다면 송신체계를 식별하기 위하여 W의 부분망의 프레임안에 있는 원천마디점주소를 리용할수 없다. 원천마디점주소는 그 자료가 어디서 이 부분망에 들어 갔는가를 표시하므로 원래의 송신체계를 식별할수 없다.

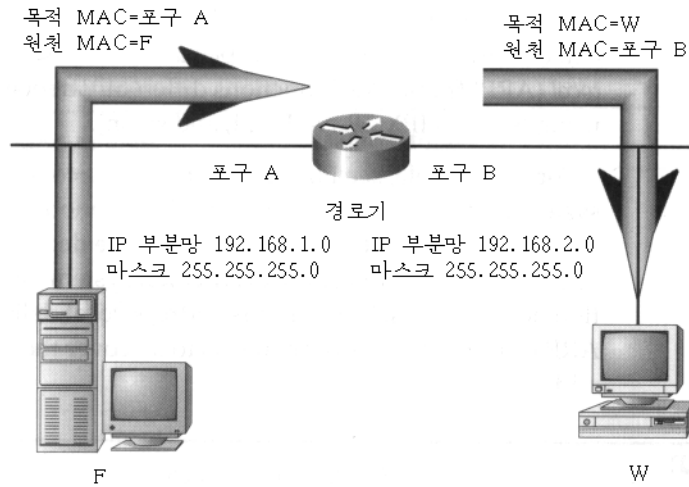



그림 3-2. 국부적통신만을 위하여 리용되는 마디점주소들

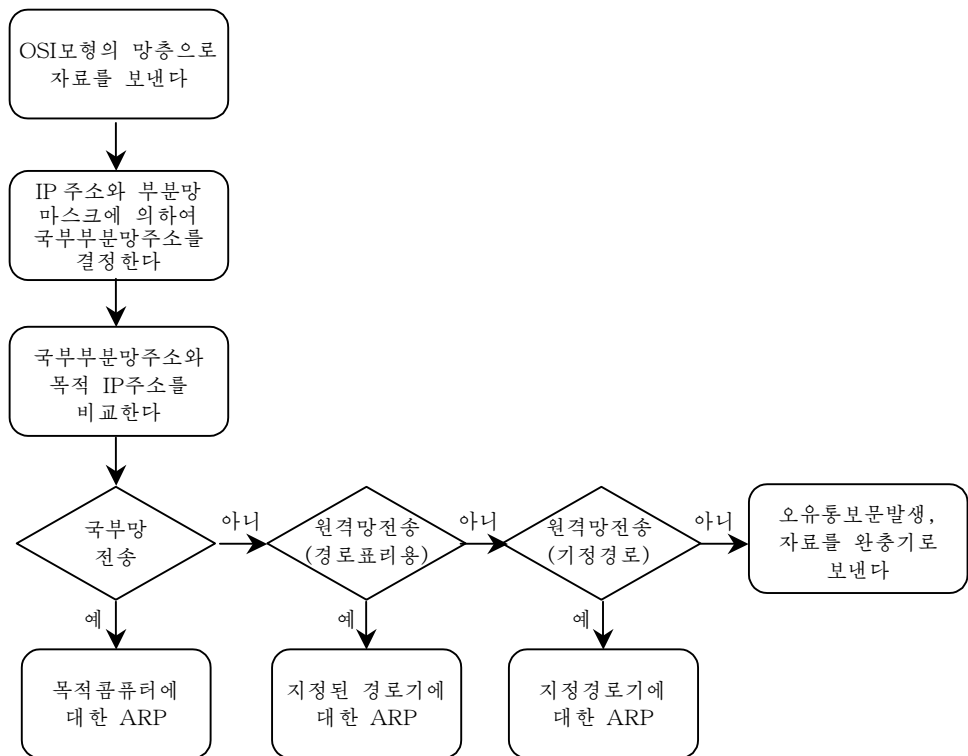



그림 3-3. ARP결정과정

F가 W와 같은 부분망에 있지 않다는것을 알게 되면 그는 경로기를 찾게 된다. 체계는 자료를 어떻게 잘 배포할것인가를 결정할 때 그림 3-3과 같은 공정을 거치게 된다. 일단 체계가 정보를 어디로 보낼것인가를 알게 되면 그것은 적당한 ARP요청을 송신한다.

모든 체계는 ARP요청을 통하여 얻은 정보를 보관할수 있다. 실례로 F가 몇초후에 W에게 다른 하나의 자료파케트를 보내려고 한다면 그는 경로기의 마디점주소를 위한 새로운 ARP요청을 전송하지 말아야 한다. 왜냐하면 이 값은 기억기에 보관될것이기때문이다. 이 기억구역을 ARP캐쉬(Cache)라고 부른다.

ARP캐쉬의 내용들은 60s동안 유지된다. 그후에 그것들은 지워 지며 다시 새로운 ARP캐쉬표에서 영구적인 내용을 만드는 정적ARP항목들을 만들수도 있다. 이렇게 하면 정적항목을 가지는 마디점들에 대하여서는 ARP요청을 전송하지 않아도 된다.

실례로 F의 기계에 경로기를 위한 정적ARP항목을 만들어 놓으면 이 장치를 찾을 때 ARP요청을 전송하지 않아도 된다. 유일한 문제는 경로기의 마디점주소가 변할 때 제기된다. 만일 경로기가 고장나서 그것을 새것으로 바꾼다면 F의 체계에 들어 가서 그 정적ARP항목을 변경시켜야 한다. 왜냐하면 그것은 새 경로기가 다른 마디점주소를 가지고 있기때문이다.

통신규약이 하는 일

한 체계가 다른 체계에 정보를 전송하려고 한다면 그것은 프레임머리부의 목적지마당에 목표체계의 마디점주소를 가지는 프레임을 만들어 보내게 된다. 이 통신방법은 해당한 위상구조의 통신규칙의 부분이다. 이 전송은 다음의 문제들을 제기한다.

- 전송체계는 프레임이 하나의 토막으로 수신되였다고 가정하면 되는가?
- 목적지체계는《나는 당신의 프레임을 송신하였다. 고맙다!》라고 응답하여야 하는가?
- 만일 응답을 보내야 한다면 매개 프레임이 자기의 답례를 요구하는가 아니면 프레임들의 한 묶음에 대하여 하나의 답례를 보내면 되는가?
- 목적지체계가 같은 국부망에 있지 않다면 자료를 어디로 보낼것인가를 어떻게 해결할것인가?
- 목적지체계가 원천체계에서 전자우편을 운영하고 파일을 전송하며 Web페지들을 돌아 다닌다면 어느 응용프로그람이 이 자료를 쓰는것인지를 어떻게 알것인가?

통신규약의 일감은 바로 이 물음들과 그리고 통신과정에 제기되는 여러 다른 문제들에 대답하는것이다. IP, IPX, AppleTalk 또는 NetBEUI에 대하여 말할 때 이것은 통신규약에 대하여 말하는것이다. 그러면 하나의 통신규약을 특징 짓는 설계서가 왜 간단히 그 위상구조에 의하여 정의되지 않는것인가?

그 대답은 다양성때문이라는것이다. IP의 통신특성들이 이써네트위상구조에 매여 있다면 모든 망토막들에서 이써네트를 리용하여야 할것이며 이것은 광지역망련결을 포함한

다. 이 봉사들이 이써네트를 위해서만 준비되여 있으므로 통표고리형이나 ATM을 리용할수 없을것이다.

여러가지 통신규칙들(통신규약들)을 정의함으로써 지금 이 규칙들은 임의의 OSI호환위상구조들에 적용될수 있다. 이것이 OSI모형이 개발되게 된 리유이다.

OSI모형

1977년에 국제규격화기구(ISO)는 서로 다른 제작자들이 내놓은 체계들사이의 통신을 개선하기 위하여 열린체계 호상접속참조모형(OSI모형)을 개발하였다. ISO는 많은 서로 다른 조직들을 대표하는 위원회로서 그것의 목적은 어떤 특정의 통신방법을 택하는것이 아니라 각이한 제작자들의 제품들이 호환성을 가지도록 보장하는 지침들을 개발하는 것이다.

ISO는 체계들사이의 통신을 간단화할것을 주장하고 있다. 자료가 먼저 정확한 체계에 도착하고 다음에 리용할수 있는 형태로 정확한 응용프로그람에 넘겨 지는것을 담보하기 위하여서는 많은 사건들이 발생하여야 한다.

규칙들의 모임은 통신과정을 간단한 구성블로크들의 모임으로 분할하여야 한다. OSI모형은 7개의 층으로 구성된다. 매층은 통신과정의 그 부분이 어떻게 기능하며 바로 웃층, 바로 아래층 그리고 다른 체계의 린접층들과 어떻게 련결되는가를 서술한다. 이것은 제작자가 일정한 준위에서 동작하는 제품을 만들게 하며 그것이 가장 넓은 응용범위에서 동작하도록 보장한다. 만일 제작자의 제품이 특정의 층에 대한 표준에 따른다면 그것은 린접층에서 동작하는 다른 제작자의 제품과 통신할수 있어야 한다.

복잡한 과정을 간단화하기

OSI 모형에 대한 한가지 비유로 집 짓는 과정을 들수 있다. 집을 짓는것은 복잡한 작업공정들로 실현될수 있는데 그것을 공정별로 분할하면 보다 쉽게 된다. 좋은 집은 기초에서 시작되며 기초를 얼마나 넓게, 얼마나 깊이 하여야 하는가에 대한 규칙들이 있다. 다음에 틀을 맞추는데 여기에도 재목이 얼마나 굵어야 하고 매개 기둥이나 들보가 받침대없이 얼마나 길게 뻗칠수 있는가에 대한 규칙들이 있다.

일단 집의 틀이 잡힌다면 벽을 쌓고 지붕을 올리며 전기체계와 수도관부설 등의 공정들이 있다. 이 복잡한 공정을 작고 여러 단순한 공정들로 나누어 진행한다면 집건설이 쉬워 지게 된다. 실례로 전기담당자의 책임은 선을 늘이고 전기코드구멍을 내는 것이지 지붕널을 잇는것이 아니다.

전체적인 구조는 매개 부분이 다른것에 의존하면서 조화롭게 짜맞춘 주단과 같이 된다.

OSI 모형은 이러한 종류의 정의와 의존성들을 설정하려고 하고 있다. 통신과정의 매 부분은 개별적인 구성블로크로 된다. 이것은 통신과정의 매 부분이 무엇을 하여야 하는가를 쉽게 결정할수 있게 한다. 또한 매 부분이 다른것과 어떻게 련결되는가를 쉽게 정의할수 있게 한다.

집을 짓는것에 비유해 말하면 재목창고에서 집건설에 쓰이는 들보를 굵기와 재질에 따라 선별하여 취급한다면 건설자들은 적당한 기초구조를 가지는 임의의 집에서 정확히 기능하는 들보들을 구할수 있을것이다.

그림 3-4는 OSI모형의 전체적인 표현이다. 매개 층의 기능을 하나씩 보기로 하자.

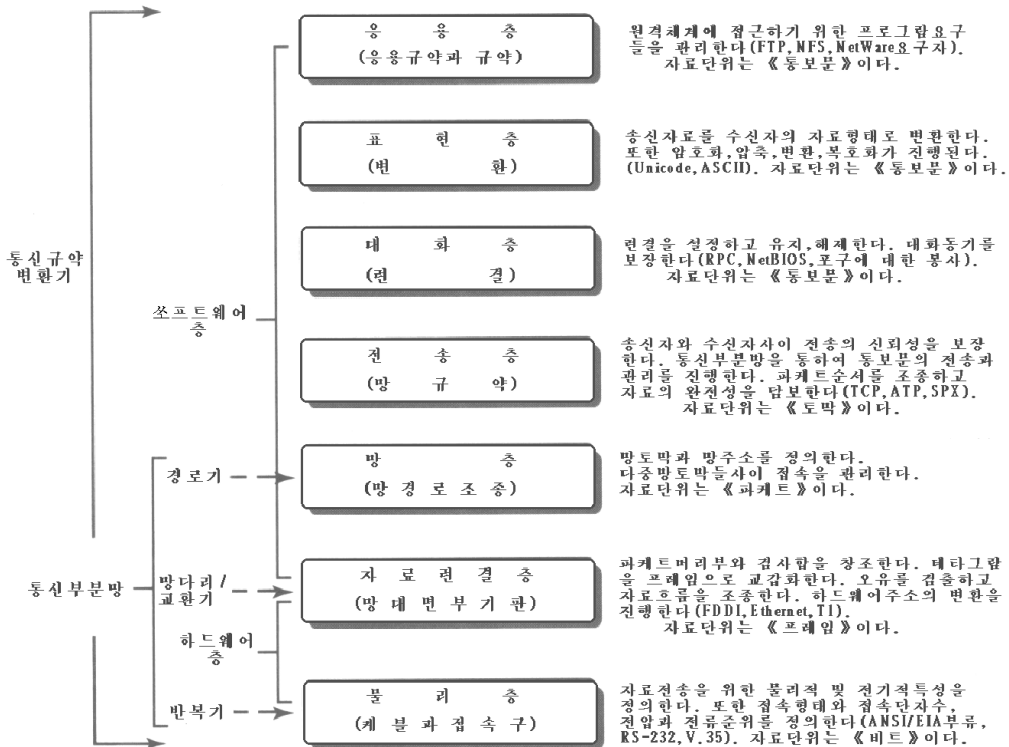



그림 3-4. OSI모형

물리층 물리층은 전송매체, 접속구, 신호임풀스들에 대하여 설명한다. 반복기나 집선기는 그것이 프레임과 관계 없고 전기신호를 증폭하고 전송하므로 물리층 장치이다.

자료련결층 자료련결층은 국부적체계들사이의 위상관계와 통신에 대한 설명을 준다. 이써네트는 다중물리층명세(꼬임쌍선, 빛케블)와 다중망층명세 (IPX, IP)를 가지고 동작하므로 자료련결층의 좋은 실례로 된다. 자료련결층은 망의 물리적측면(케블이나 수자식임풀스)을 쏘프트웨어의 추상세계와 자료흐름과 련결시키는 《세계들사이의 문》이다. 망다리와 교환기는 프레임관련이므로 자료련결층장치로 간주된다. 이것들은 둘 다 자료흐름을 조절하는데서 프레임머리부의 정보를 리용한다.

망층 망층은 서로 다른 망에 있는 체계들이 어떻게 서로 찾는가를 서술한다. 그것은 또한 망주소들을 정의한다. 망주소는 물리적으로 련결된 체계들의 한 집단에 배당된 이름 또는 번호이다.

주 의

망주소는 망관리자에 의하여 배당되며 매 망기판에 배당되는 MAC주소와 혼돈하지 말아야 한다. 망주소의 목적은 장거리자료전송을 쉽게 하기 위한것이다. 그것의 기능은 편지를 부칠 때 우편번호를 써넣는것과 류사하다.

IP, IPX 그리고 AppleTalk의 데타그람배포규약(DDP)은 모든 망층기능의 실례들이다. 봉사 및 응용프로그람의 효과성은 이 준위에서 지적된 기능에 기초하고 있다.

주 의

망층기능에 대한 상세한것을 알려면 이 장의 소제목 《망층에 대한 보충》을 보시오.

전송층 전송층은 자료의 실제적인 조작을 취급하며 망을 통한 자료배포를 준비한다. 만일 자료가 하나의 프레임으로서는 너무 크다면 전송층은 그것을 보다 작은 토막들로 분할하고 순서번호를 붙인다. 순서번호는 다른 수신체계의 전송층에서 그 자료를 원래의 내용으로 재조립할수 있게 한다. 자료련결층은 모든 프레임들에 대하여 CRC검사를 수행하지만 전송층은 모든 자료들이 수신되고 쓸수 있다는것을 담보하기 위하여 여벌검사로서 동작할수 있다. 전송층기능의 실례는 IP의 전송조종규약(TCP), 사용자데타그람규약(UDP), IPX의 순서파케트교환(SPX), AppleTalk의 ATP들이다.

대화층 대화층은 둘 또는 그이상의 체계들사이에서 련결을 설정하고 유지하는것을 취급한다. 그것은 특정봉사형태에 대한 질문이 정확히 만들어 진다는것을 담보한다. 실례로 자기의 Web열람기로 한 체계에 접근하려고 한다면 이 두 체계에서 대화층들은 전자우편이 아니라 HTML페지들을 받는다는것을 함께 담보하도록 동작한다. 만일 체계가 여러개의 망응용프로그람들을 돌리고 있다면 이 통신들을 순서대로 유지하고 들어 오는 자료가 정확한 응용프로그람에로 간다는것을 담보하는것은 대화층까지이다. 사실상 대화층은 하나의 봉사안에서 일의적인 대화를 유지한다. 실례로 같은 시간에 같은 Web싸이트로부터 두개의 다른 Web페지를 내리받기한다는것을 생각해 보시오(같은 콤퓨터로부터). 대화층은 매 파일전송의 완전성을 유지하며 두 자료흐름이 섞이지 않도록 수신체계에서 혼돈되지 않음을 담보한다.

표현층 표현층은 자료가 체계에서 돌아 가는 응용프로그람에 리용가능한 형태로 접수되는것을 담보한다. 실례로 인터네트상에서 암호화된 통신을 리용하여 통신하고 있다면 표현층은 이 정보를 암호화 및 복호화할 책임을 진다. 대부분의 Web열람기들은 인터네트에서 금융업무를 수행하기 위하여 이러한 기술을 지원한다. 자료 및 언어번역도 이 준위에서 수행된다.

응용층 응용층이라는 말은 이것이 사용자가 체계에서 돌리고 있는 실제적인 프로그람을 서술하는것이 아니므로 좀 오해를 줄수 있다. 이 층은 오히려 망자원에

로의 접근이 언제 요구되는가를 결정하는데 책임이 있는 층이다. 실례로 Microsoft Word는 OSI모형의 응용층에서 기능하지 않는다. 만일 한 사용자가 봉사기에 있는 자기의 홈등록부로부터 하나의 문서를 검색하려고 한다면 응용층망쏘프트웨어는 원격체계에 그의 요구를 전송할 책임을 가진다.

OSI모형은 어떻게 동작하는가

이 층들이 어떻게 함께 동작하는가를 보기 위하여 하나의 실례를 고찰하자. 만일 자기의 문서처리프로그람을 리용하고 있고 원격봉사기에 있는 자기의 홈등록부로부터 파일 resume.txt를 검색하려고 한다고 가정하자. 체계에서 돌아 가는 망쏘프트웨어는 다음의 서술과 같이 반응할것이다.

파일요청을 형식화하기

응용층은 원격파일체계로부터 정보를 요청하고 있다는것을 검출한다. 그것은 resume.txt가 있는 체계에로 가는 하나의 요청을 형식화한다. 이 요청을 만들면 응용층은 다음의 처리를 위하여 그것을 표현층에 보낸다.

표현층은 이 요청을 암호화할 필요가 있는가 또는 어떤 형식의 자료변환을 할것인가를 결정한다. 일단 이것이 결정되고 완성되면 표현층은 그것에 원격체계의 표현층을 통과하는데 필요한 어떤 정보들을 추가하고 그 파케트를 대화층에로 보낸다.

대화층은 어느 응용프로그람이 그 정보를 요구하고 있는가를 검사하고 원격체계로부터의 어떤 봉사가 요청되고 있는가를 확인한다(파일접근). 대화층은 원격체계가 어떻게 이 요청을 처리할것인가를 알고 있다는것을 담보하기 위해 그 요청에 정보를 첨가한다. 다음에 전송층에로 이 모든 정보들을 보낸다.

전송층은 그것이 원격체계와 믿음성 있는 련결을 가지고 있다는것을 담보하여 정보들을 분할하여 프레임으로 포장하는 공정을 시작한다. 하나의 프레임이상이 요구된다면 정보는 분할되고 매 블로크에 순서번호가 배당된다. 이 순서화된 정보묶음이 한번에 하나씩 망층으로 내려 간다.

망층은 전송층으로부터 정보블로크들을 받고 망주소를 첨가한다. 이것은 자료련결층으로 내려 가는 매 블로크에 대하여 수행된다.

자료련결층에서 블로크들은 개별적인 프레임들로 포장된다. 그림 3-5에서 보여 준것처럼 매 이전층들에서 보충된 모든 정보는(실제적인 파일요청도 함께) 이써네트프레임의 46-1500byte 크기에 맞아야 한다. 자료련결층은 다음에 원천 및 목적지MAC주소로 구성된 프레임머리부를 첨가하고 이 정보를 리용하여(자료마당의 내용에 따라) CRC꼬리부를 만든다. 자료련결층은 다음에 망에서 리용되는 위상구조규칙에 따라 그 프레임을 전송할 책임을 진다. 위상구조에 따라 이것은 망우에서 조용한 순간동안 듣기, 통표기다림 또는 전송전의 특정한 시간분할대기 등을 의미할수 있다.

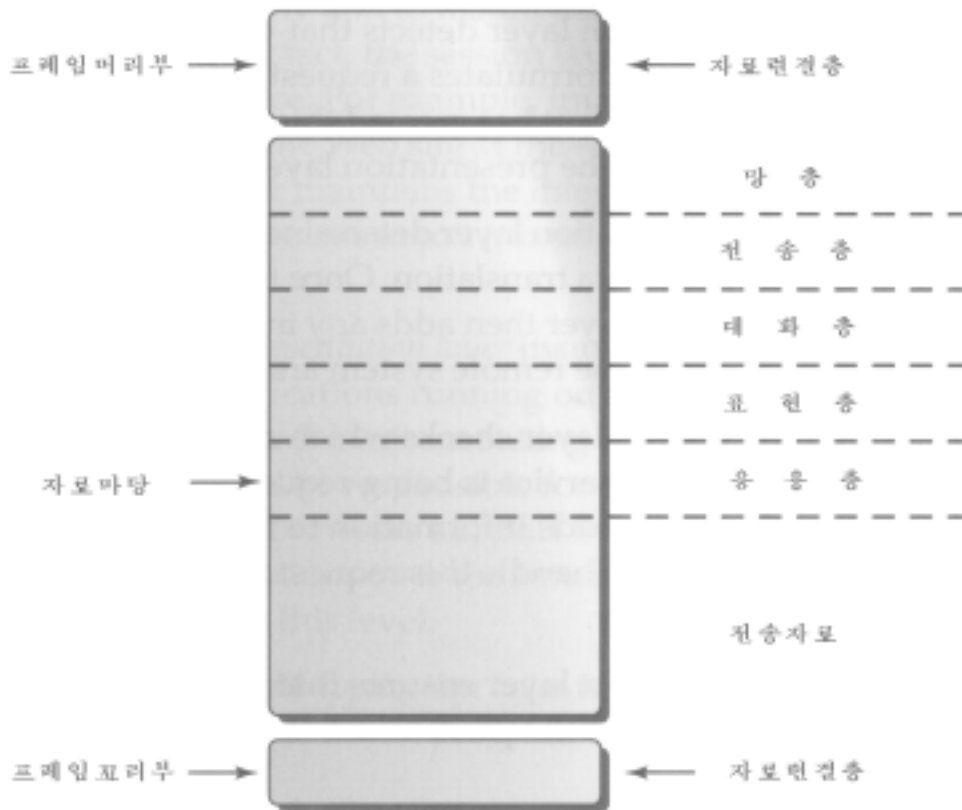



그림 3-5. 프레임에서 매 층의 정보의 위치

주 의

물리층은 프레임에 어떤 정보도 첨가하지 않는다.

물리층은 원천으로부터 목적지에로 정보를 나르는 책임을 진다. 물리층은 프레임에 따라 정보를 가지고 있지 못하므로 자료련결층으로부터 전송된 수자신호임풀스들을 그저 통과시킨다. 물리층은 두개의 매 체계사이에 련결이 이루어 지는 매체로서 원격체계의 자료련결층에로 신호를 나르는 책임을 진다.

이로서 콤퓨터는 자료요청(《나에게 resume.txt의 복사본을 보내시오.》)을 성과적으로 형식화하였으며 그것을 원격체계에 전송하였다. 이 점에서 원격체계는 류사하지만 반대방향인 과정을 수행한다.

원격체계에서 자료를 받기

원격체계의 자료련결층은 전송된 프레임을 읽어 들인다. 그것은 머리부의 목적지마당의 MAC주소가 자기의것이라는것을 알고 자기가 이 요청을 처리해야 한다고 인정한다. 그 프레임에 대한 CRC검사를 진행하고 그 결과를 프레임꼬리부에 보관된 값과 비교한다. 이 값이 일치하다면 자료련결층은 머리부와 꼬리부를 떼버리고 그 자료련결층은 원천체

계에 또 하나의 프레임을 보낼것을 요구하는 요청을 보낸다.

원격체계의 망층은 올라 온 정보를 분석한다. 목적지쏘프트웨어주소가 자기것임을 알게 된다. 이 분석이 끝나면 망층은 이 준위와 관련된 정보를 제거하고 나머지를 전송층에 보낸다.

전송층은 그 정보를 받고 분석한다. 만일 파케트순서화가 리용되였다는것을 발견하면 자료가 다 수신될 때까지 대기한다. 만일 자료의 일부가 손실되였다면 전송층은 순서정보를 리용하여 원천체계에서 보낼 하나의 응답을 형성하는데 잃어 진 자료토막을 다시 전송할것을 요구한다. 모든 자료가 수신되면 전송정보들을 떼버리고 대화층에 그것을 올려 보낸다.

대화층은 정보를 받고 그것이 정당한 련결로부터 온것인가를 확인한다. 검사가 제대로 되면 대화층정보를 떼버리고 그 요청을 표현층에 보낸다.

표현층은 그 정보를 받고 분석한다. 요구되는 어떤 변환 또는 부호화를 수행한다. 변환이나 부호화가 끝나면 표현층정보를 떼버리고 그 요청을 응용층에 올려 보낸다.

응용층은 그 체계에서 돌아 가는 정확한 과정이 그 자료요청을 접수한다는것을 담보한다. 이것이 파일요청이므로 그것은 파일체계접근에 책임이 있는 어느 공정에 보내진다. 이 공정은 요청된 파일을 읽고 그것을 응용층에 보낸다. 이 점에서 매개 층을 통하여 정보를 보내는 전체 과정이 반복된다.

망층에 대한 보충

앞에서 언급되였지만 망층은 론리적망들사이에서의 정보의 전송을 위하여 리용된다.

주 의

론리적망이란 간단히 망관리자에 의하여 공통망주소가 할당된 체계들의 집단이다. 이 체계들은 공통적인 지역 또는 배선중심을 공유하고 있는것으로 하여 함께 클라스터화될수 있다.

망주소들

망주소에 대하여 리용되는 술어는 리용되는 통신규약에 따라 다르다. 리용되는 통신규약이 IPX라면 론리적망은 간단히 하나의 망주소라고 한다. IP이면 그것은 부분망, AppleTalk이면 지역(zone)이라고 부른다.

주 의

NetBEUI는 전송층, 망층 그리고 자료련결층(그것의 LLC부분)의 겹침으로 볼수 있으나 NetBIOS와 NetBEUI는 경로조종불가능한 규약들이다. 이것들은 망번호를 리용하지 않으며 론리적망토막들사이에서 정보를 전파할 능력을 가지지 않는다. 경로조종불가능한 통신규약은 모든 체계들이 국부적으로 련결될것을 요구하는 통신규칙들의 모임이다. 경로조종불가능한 통신규약은 국부망들사이로 움직일 직접적인 방법을 가지고 있지 못하다. NetBIOS프레임은 어떤 형태의 도움이 없이 하나의 경로기를 통과할수 없다.

경 로 기

경로기는 론리적망들을 련결하는데 리용된다. 그러므로 그것들은 때로 IP세계에서 관문(게이트웨이)이라고 부른다. 그림 3-6은 하나의 망에 경로기를 추가한 결과를 보여 준다. 그 장치의 어느 한쪽에 있는 통신규약들은 일의적인 론리적망주소를 리용하여야 한다는것에 주목하기 바란다. 국부망이 아닌 체계에서 요구되는 정보는 그 체계가 있는 론리적망에로 경로조종되여야 한다. 한 론리망으로부터 다른 망에로 경로기를 건너 가는 동작을 도약(hop)라고 한다. 통신규약이 경로기를 도약할 때 그것은 량쪽에서 일의적인 론리망주소를 리용하여야 한다.

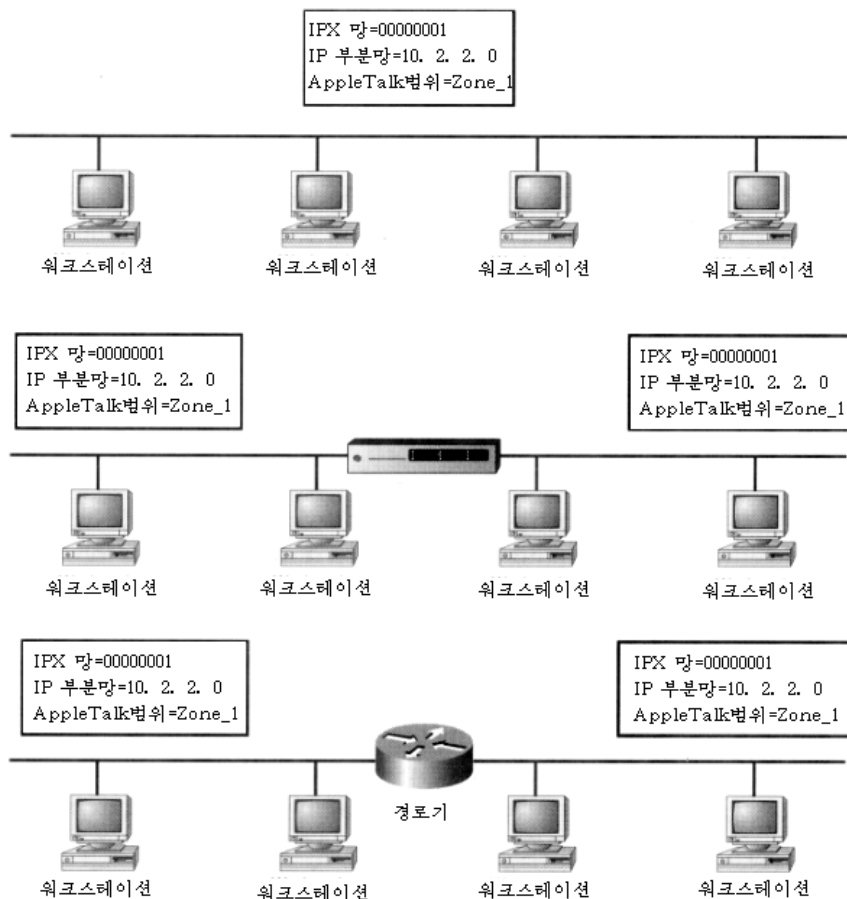



그림 3-6. 망에 경로기를 추가한 결과

그러면 한 론리망토막에 있는 체계가 그 망에 다른 론리토막들이 있다는것을 어떻게 알수 있겠는가? 경로기는 원격망들을 찾아 가기 위한 경로를 서술하는 정보를 가지고 정적으로 프로그람화될수도 있고 또는 경로조종정보규약(RIP)과 같은 특수한 형태의 프레임을 리용하여 알려 진 망들에 대한 정보를 중계할수도 있다. 경로기는 이 프레임들과

정적인 항목들을 리용하여 경로조종표라고 부르는 망의 계획을 만든다.

주 의

경로조종표는 어느 론리망이 정보전송에 준비되여 있고 어느 경로기가 그 망에 정보를 넘길수 있는가를 경로기에게 보여 준다.

경로조종표

경로조종표를 도로지도와 같이 생각할수 있다. 도로지도가 도시의 거리들을 다 보여주는것과 같은 방법으로 경로조종표는 모든 국부망들의 통로를 가지고 있다.

이 매개 경로기들이 서로 통신하며 누가 어디에 련결되는가를 알게 하는 방법이 없다면 론리망토막들사이의 통신은 불가능할것이다.

한 망으로부터 다른것에로 정보를 경로조종하는데는 3가지 방법이 있다.

- 정적방법
- 거리벡토르법
- 련결상태법

매개 통신규약은 자기의 경로조종기능제공방법을 가지고 있으므로 매 실현은 이 세가지 류형중 하나로 갈라 지게 된다.

정적경로조종

정적경로조종은 한 체계로부터 다른것에로 정보를 보내는 가장 간단한 방법이다. 정적경로조종에서는 특정의 경로기를 특정의 망에로 경로조종하는 점으로 정의한다. 정적경로조종은 경로기가 경로정보를 바꿀것을 요구하지 않는다. 그것은 특정의 망에 있어서 특정의 경로기에로의 통신량한계를 지시하는 구성파일에 의존한다. 이것은 물론 통신하려고 하는 모든 국부망들을 미리 결정할수 있다는것을 가정한다. 이것이 쉽지 않을 때(실례로 인터네트상에서 통신할 때) 미리 정의되지 않은 망들에 대한 모든 통신량들을 접수하기 위한 기정의 경로기로 하나의 경로기가 선정되게 된다. 정적경로조종이 리용될 때 대부분의 콤퓨터들은 기정경로기만을 위한 항목을 수신한다.

실례로 어떤 체계를 갈리프레이라고 하는 경로기로 지적하는 기정경로를 가지도록 구성한다고 가정하자. 체계가 망층으로 정보를 통과시킬 때 그것은 목적지체계의 론리적망을 분석할것이다. 만일 그 체계가 같은 론리망에 위치하고 있다면 자료련결층은 그 체계의 MAC주소를 첨부하고 그 프레임을 전송한다. 그 체계가 다른 망에 위치하고 있다면 자료련결층은 갈리프레이를 위한 MAC주소를 리용하고 그 프레임을 그것에 전송한다. 그 프레임이 자기의 최종목적지에로 가도록 담보하는것은 갈리프레이의 책임이다.

이러한 경로조종방법의 우점은 간단하고 부차적소비가 적은것이다. 나의 콤퓨터는 어떤 다른 론리망이 준비되여 있고 어떻게 거기로 갈것인가를 알 필요가 없다. 두가지

문제거리가 있는데 국부적배포와 갈리프레이에게로의 배포이다. 이것은 최종목적지에로의 경로가 하나만 있을 때에는 효과적일수 있다. 실례로 대부분의 기관들은 하나의 인터네트련결만을 가진다. 이 련결에 가까운 경로기에로 모든 IP통신량을 지적하는 하나의 정적경로를 설정하면 모든 프레임들이 적당히 배포된다는것을 가장 쉽게 담보할수 있다. 모든 경로조종정보들이 시작시에 구성되므로 경로기는 경로조종정보를 다른 경로기들과 공유하지 않아도 된다. 매개 체계는 다만 자기의 다음번 기정경로에 넘겨 주는 정보만을 관심한다. 이때에는 자기망을 통하여 전송되는 동적경로조종프레임들을 가지지 않아도 된다. 왜냐하면 매개 경로기는 정보를 어디로 넘겨야 한다는것을 미리 설정하고 있기때문이다.

정적경로조종은 리용하기 쉽지만 그것의 응용범위를 크게 제한하는 몇가지 결함을 가지고 있다. 여분의 경로들이 있을 때 또는 여러개의 경로기들이 같은 망에서 리용될 때 동적경로정보를 교환할수 있는 경로조종방법을 쓰는것이 보다 효과적이다. 동적경로조종에서는 경로조종표가 동작중에 만들어 지는데 이로 하여 장치적고장들을 보상할수 있다. 거리벡토르법과 련결상태경로조종에서는 경로조종표가 항상 최신의것으로 되도록 하기 위하여 동적경로정보를 리용한다.

정적경로조종보안

정적경로조종은 보존성이 높으므로 경로조종표를 만드는데서는 가장 안전한 방법이라고 볼수 있다. 동적경로조종은 경로조종표가 망에 있는 장치들에 의하여 동적으로 갱신되도록 한다. 공격자는 경로기에 부정확한 경로정보를 넣기 위하여 이 성질을 리용할수 있다. 사실상 동적경로조종규약을 리용하면 공격자는 하나의 경로기에만 가짜정보를 넣으면 된다. 이 오염된 경로기는 이 가짜정보를 망의 다른 부분들에도 퍼뜨리게 된다. 매개 정적경로기는 자기의 경로조종표를 보존할 책임이 있다. 이것은 하나의 경로기가 오염되여도 공격의 효과가 다른 경로기들에로 자동적으로 퍼지지 않는다는것을 의미한다. 정적경로조종을 리용하는 경로기는 ICMP방향돌림공격에는 취약할수 있지만 그것의 경로조종표는 틀린 경로정보의 전파에 의하여 파괴될수 없다.

주 의

ICMP에 대한 내용을 알려면 제5장의 《파케트려과 ICMP》를 보기 바란다.

거리벡토르경로조종

거리벡토르법은 가장 오래고 널리 쓰이는 경로조종표작성법이다. 경로조종규약(RIP)은 이 거리벡토르법에 기초하고 있다. 여러해동안 거리벡토르법은 유일한 동적경로조종방법으로 쓰이였으며 많은 망들에서 사용되였다.

거리벡토르법에서는 간접적인 정보들로 표를 구성한다. 하나의 경로기는 다른 경로기들이 공시하는 표들을 보고 자기의 표를 만들기 위하여 공시된 도약값에 간단히 1을 더한다. 이 방법에서 매개 경로기는 자기의 경로조종표를 1min에 한번씩 방송한다.

거리벡토르법에 의한 망정보의 전파

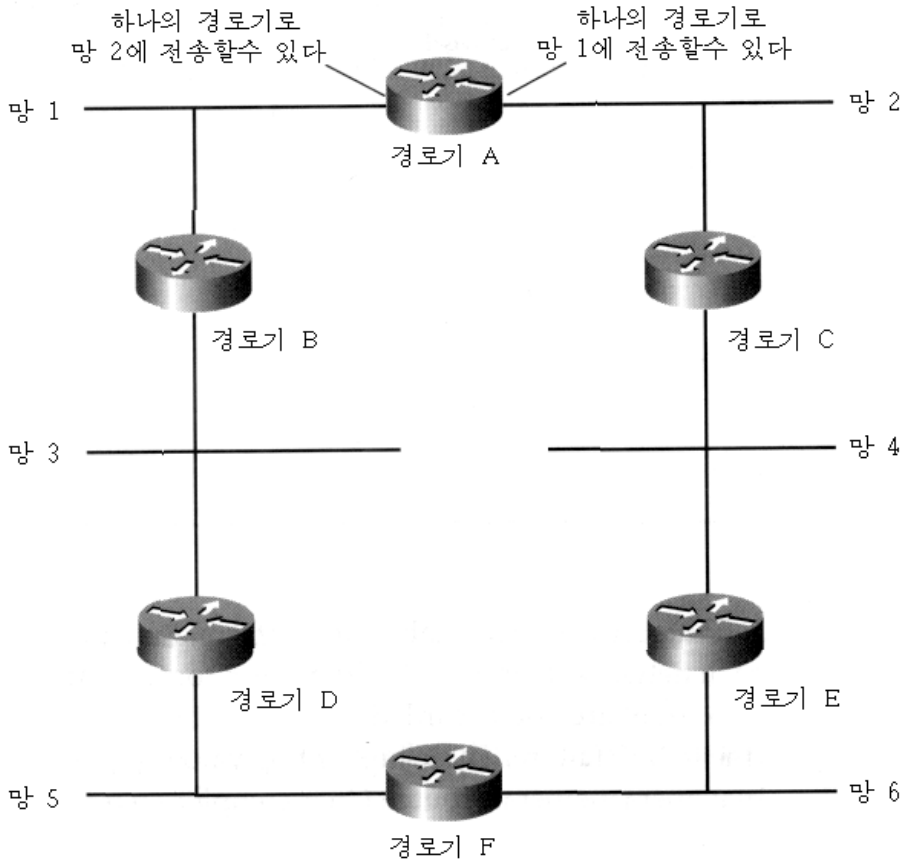



그림 3-7. 동적으로 경로조종표를 만들기 위한 경로화된 망

그림 3-7은 망정보의 전파가 거리벡토르에 따라 어떻게 진행되는가를 보여 준다.

경로기 A가 현재 주목되는 중인데 두개의 망(1과 2)이 그것에 붙어 있으므로 매개에 1의 도약값을 배당하여 그것들을 자기의 경로조종표에 기입한다. 이 정보는 그 경로기가 아니라 다른 붙어 있는 망들에 상대적인것이므로 도약값은 0이 아니라 1이다.

실례로 그 경로기가 망 2우에서 망 1로 가는 경로를 공시하고 있다면 망 2로부터 망 1로 정보를 보내는 임의의 체계는 거기로 가기 위하여 하나의 도약만큼 옮겨 가므로 하나의 도약이 적당하다. 경로기는 보통 그 망자체에 직접 붙어 있는 망에 대한 경로점은 공시하지 않는다. 이것은 그 경로기가 망 1자체에서는 《나는 한 도약으로 망 1에 도달할수 있다.》는 RIP프레임을 전송하지 말아야 한다는것을 의미한다.

경로기 A는 매개 망에 하나씩 두개의 RIP파케트를 보내여 어떤 다른 장치들이 그것이 제공할수 있는 련결성을 알도록 한다. 경로기 B와 C가 이 파케트들을 받으면 그것들은 자기의 RIP파케트로 응답한다. 망은 이미 돌아 가고 있다는것을 상기하여야 한다. 이것은 모든 다른 경로기들이 이미 자기의 표들을 만들 준비가 되여 있다는것을 의미한

다. 이 다른 RIP파케트들로부터 경로기 A는 표 3-2에 보여 준것과 같은 정보들을 수집한다.

표 3-2　　　　　　경로기 A가 받은 경로정보

경로기	망	거기로 가는 도약수
B	3	1
B	5	2
B	6	3
B	4	4
B	2	5
C	4	1
C	6	2
C	5	3
C	3	4
C	1	5

경로기 A는 다음에 이 정보들을 분석하여 매개 망에로의 가장 낮은 도약수를 뽑아내여 자기의 경로조종표를 만든다. 큰 도약수를 요구하는 경로들은 무시되는데 련결고장으로 하여 또 다른 경로가 필요한 경우에는 남겨 둔다. 경로기의 표준동작에서는 이보다 큰 도약값들은 무시된다. 완성된 표를 표 3-3에 보여 준다.

표 3-3　　　　　　경로기 A의 경로조종표

망	거기로 가는 도약수	다음번 경로기
1	1	직접련결
2	1	직접련결
3	2	B
4	2	C
5	3	B
6	3	C

지금까지 한것은 매개 망에로의 가장 낮은 도약값을 뽑아 내고 공시된 값에 1을 더한것이다. 표가 완성되면 경로기 A는 다시 두개의 RIP파케트를 방송하여 이 새로운 정보들을 공시한다.

그러면 경로기 B와 C는 망에 새로운 경로기가 있다고 보고 자기들의 경로조종표를 재평가하게 된다. 경로기 A가 초기화되기전의 경로기 B의 표를 표 3-4에 보여 준다.

표 3-4　　경로기 A가 초기화되기전의 경로기 B의 경로조종표

망	거기로 가는 도약수	다음번 경로기
1	1	직접련결
2	5	D
3	1	직접련결
4	4	D
5	2	D
6	3	D

이제 경로기 A가 동작한후에 경로기 B는 자기의 표를 갱신한다.

표 3-5　　경로기 A가 초기화된후의 경로기 B의 경로조종표

망	거기로 가는 도약수	다음번 경로기
1	1	직접련결
2	2	A
3	1	직접련결
4	3	A
5	2	D
6	3	D

여기까지 오기에는 같은 론리망에서 두개의 RIP를 사용하였다. 처음으로 경로기 A가 하나의 RIP를 경로기 B로 보냈을 때에는 망 2에 대해서만 알게 된다(그림 3-7). 그리고 경로기 C가 하나의 응답RIP를 보낸후에야 경로기 A는 두번째 RIP프레임을 경로기 B에 보내여 새로운 정보를 리용하게 한다. 표 3-5는 직접적인 공통망정보만(망 1) 삭제되고 있는것으로 방송되게 된다. 이것은 경로기 A가 경로기 C로부터 얻은 정보를 가지고 경로기 B를 갱신하고 있는 동안 그것은 그 경로기(경로기 B)가 원래 보낸 경로정보를 되중계하고 있다는것을 의미한다. 유일한 차이는 경로기 A는 경로기 B가 보낸 매개 도약수를 1만큼 증가시켰다는것이다. 그 도약값은 경로기 B가 자기의 표에서 현재 가지고 있는것보다 크므로 경로기 B는 이 정보를 무시하게 된다.

경로기 C는 류사한 과정으로 경로기 A로부터 받은 정보에 따라 자기의 표를 조절한다. 그도 역시 같은 망에서 두개의 RIP로 요구하여 전체 망에 대한 완전한 시각을 얻게 되며 자기의 표의 변경을 완성하게 된다.

다음에 이 변화는 망을 통하여 전파되기 시작한다. 경로기 B는 경로기 D를 갱신하며 이 동작은 모든 경로기들이 새로운 망에 대한 정확한 시각을 얻을 때까지 계속된다. 모든 경로기들이 표변경을 완성하는데 걸리는 시간을 수렴시간이라고 한다. 모든 경로기들이 새로운 표를 가지고 안정하게 될 때까지 경로조종표는 류동상태에 있게 되므로 이 수렴시간은 중요한 지표로 된다.

경 고

큰 망에서는 RIP갱신이 분당 1~2회인것으로 하여 수렴시간이 매우 길수 있다.

거리벡토르경로조종문제

거리벡토르경로조종표는 거의 완전히 간접정보에 의하여 만들어 진다는것을 아는것이 중요하다. 어떤 경로기에서 도약수가 1보다 큰 어떤 경로는 그것이 다른 경로기로부터 무엇을 배웠는가에 기초하고 있다. 경로기 B가 경로기 A에게 자기가 망 5에는 두개의 도약으로, 망 6에는 3개의 도약으로 도달할수 있다고 말할 때 그것은 경로기 D로부터 받은 정보의 정확성을 완전히 믿고 있는것이다.

그림 3-8은 아주 간단한 한 망배치를 보여 준다. 그것은 3개의 경로기에 의하여 분리된 4개의 론리망으로 구성되여 있다. 일단 수렴점에 도달하면 매 경로기는 그 표와 같이 경로조종표를 만들것이다.

망	호프수	다음경로기
1	1	직접전송
2	1	직접전송
3	2	B
4	3	B

망	호프수	다음경로기
1	2	A
2	1	직접전송
3	1	직접전송
4	2	C

망	호프수	다음경로기
1	3	B
2	2	B
3	1	직접전송
4	1	직접전송

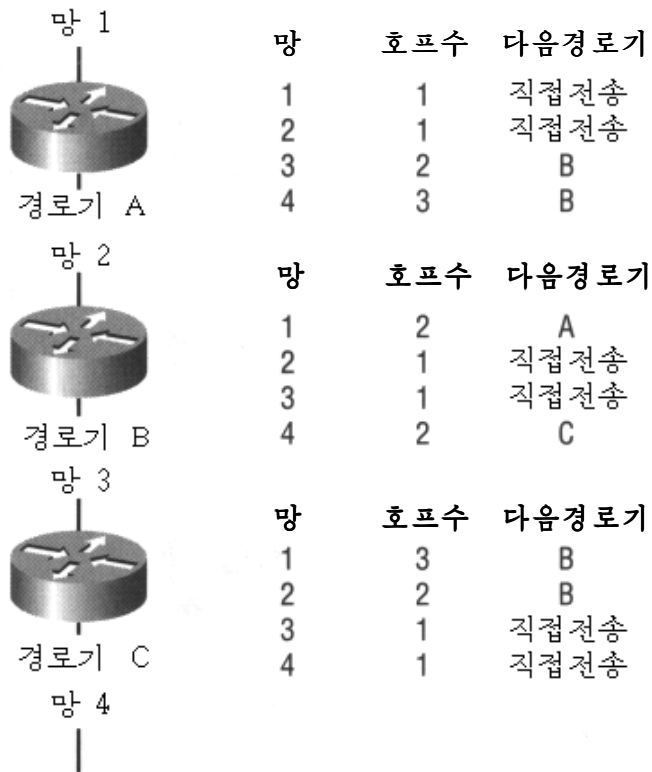



그림 3-8. 도식화된 망이 주어 지면 매개 경로기는 자기의 경로조종표를 구성한다.

이제 경로기 C가 타서 떨어 져 나갔다고 가정하자. 이렇게 되면 망 4는 모든 다른 망토막들에 도달할수 없게 된다. 경로기 B는 경로기 C가 떨어 져 나간것을 알게 되면 자기가 이전에 받은 RIP정보들을 다시 검토하여 다른 하나의 경로를 찾는다. 이것은 거

리벡토르경로조종이 오동작하기 시작하는 과정이다. 경로기 A는 자기가 망 4에 3개의 도약으로 갈수 있다고 공시하였으므로 경로기 B는 이 값에 1을 더하고 자기가 경로기 B를 통하여 망 4에 도달할수 있다고 가정한다. 이렇게 간접정보에 의존하는것은 문제를 발생시킨다. 경로기 C가 고장나면 경로기 B는 망 4에 경로기 A를 통하여 도달할수 없는것이다.

그림 3-9에서 볼수 있는바와 같이 경로기 B는 지금 자기가 4개의 도약으로 망 4에 도달할수 있다고 공시하기 시작한다. RIP프레임은 하나의 경로기가 어떻게 가는가 하는것은 알지 못하고 다만 그것이 가능하며 거기에 가는데 몇개의 도약이 필요하다는것만을 식별한다. 경로기 A가 망 4에 어떻게 간다는것을 알지 못하므로 경로기 B는 원래 자기가 보낸 경로정보에 경로기 A가 의존하고 있다는 생각은 가지지 못한다.

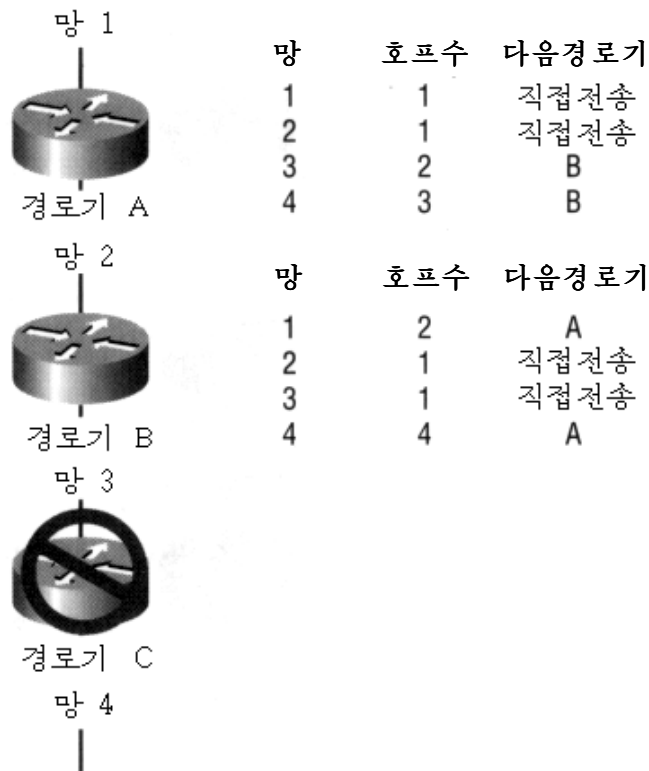



그림 3-9. 경로기 B는 A의 정보를 틀리게 믿고 자기의 표를 갱신한다.

경로기 A는 경로기 B로부터의 갱신 RIP를 받고 망 4에로의 도약수가 2로부터 4로 증가하였음을 알게 된다. 그러면 경로기 A는 자기의 표를 그것에 따라 조절되고 자기가 5개의 도약으로 망 4에 도달한다는것을 공시하기 시작한다. 그러면 경로기 B는 다시 망 4에로의 도약수를 하나만큼 증가시킨다.

주 의

이 현상은 두 경로기가 자기들의 도약수를 무한히 계속 증가시키므로 무한대셈세기라고 부른다. 이 문제로 하여 거리벡토르경로조종방법에서는 최대도약수를 15로 제한한다. 16이상의 도약수를 가지는 경로는 도달불가능한것으로 간주되며 경로조종표로부터 제거된다.

RIP갱신은 분당 한번 또는 두번만 전송된다. 이것은 경로기들이 망 4에 도달할수 없다는것을 알기까지 1min이상 걸린다는것을 의미한다. μs단위로 프레임전송을 진행하는 기술에서 1min이상의 시간은 통신에 파괴적손실을 주는 대단히 큰 시간이다. 실례로 경로기들이 수렴하려고 하는동안 망 2에서 무슨 일이 생기는가를 보기로 하자.

경로기 C가 떨어 져 나가면 경로기 B는 경로기 A를 통하여 또 하나의 경로를 가지고 있는것으로 가정한다. 그것이 받는 파케트들은 오유검사되고 경로기 A로 보내진다. 경로기 A가 그 프레임을 받으면 다시 오유검사를 진행하고 자기의 표를 참고하고는 그것이 망 4로 가기 위해 경로기 B로 가야 한다는것을 알게 된다. 경로기 B는 그 프레임을 수신하면 그것을 다시 경로기 A에 보내게 된다.

이것을 경로순환고리라고 한다. 이것을 《뜨거운 감자》문제라고도 하는데 매개 경로기는 그 프레임을 전송할 책임이 다른 경로기에 있다고 보고 그것을 서로 도로 넘겨주는것이다. 실례에서는 하나의 프레임만을 취급하지만 망 4로 가는 통신량이 적지 않다고 보면 막대한 통신자원이 손실될것이다.

다행히도 망층에는 이 문제를 해결할수 있는 방법이 있다. 매개 경로기가 프레임을 다룰 때 그 프레임안에 있는 도약계수기를 1만큼 감소시켜야 한다. 도약계수기는 그 정보가 몇개의 경로기를 통과하겠는가를 기록하기 위한것이다. RIP프레임에서와 마찬가지로 이 계수기는 15라는 최대값을 가진다. 그 정보가 16번째로 처리될 때(계수기가 0으로 떨어 질 때) 그 경로기는 그 정보가 전송불가능하다고 판단하고 그것을 제거해 버린다.

이 16이라는 도약제한은 보통의 기업망에서는 문제가 아니지만 큰 망에서는 중요한 문제로 된다. 실례로 인터네트와 같은 큰 망에서 RIP가 사용된다면 인터네트의 어떤 부분들은 많은 자원에 도달할수 없을것이다.

RIP와 관련한 보안

RIP경로조종표는 간접정보에 기초하여 만들어 진것외에 또 이 정보는 실제적으로 확인되지 않는다. 실례로 경로기 B가 어떤 주어 진 망에로의 최량의 경로를 가지고 있다고 주장하면 다른 경로기들은 이 정보를 확인하지 않는다. 실지로 그것들은 이 정보가 경로기 B로부터 보낸것인지 그리고 경로기 B가 존재하는지조차 확인하지 않는다.

이러한 확인이 없는것은 보안상의 약점이라고 말할수 있다. 가짜경로정보를 퍼뜨리고 전체 망이 잘못 동작하게 만드는것은 전혀 어려운것이 아니다. 이것은 한사람의 심술궂은 사용자가 전체 망을 위한 통신을 어떻게 중단시킬수 있는가 하는 명백한 실례이다.

이상에서 본 이러한 보안관련문제들과 그리고 또 다른 문제들로 하여 많은 회사나 기관들은 정적경로조종을 리용하거나 OSPF(Open Shortest Path First)와 같은 련결상태경로조종규약을 리용하고 있다. OSPF에서는 RIP에서의 수렴문제와 같은 많은 문제들을 제

거하였을뿐아니라 표에 인증문제를 도입하고 경로기가 경로갱신에 참가하기 위해서는 통과암호를 사용하도록 요구하고 있다. 전혀 결함이 없는것은 아니지만 이 방법은 동적경로조종환경에서 보안을 크게 증가시킨다.

련결상태경로조종

련결상태경로기는 거리벡토르법과 류사하게 동작하나 몇가지 중요한 례외를 가지고 있다. 가장 중요한것은 련결상태경로기는 경로조종표를 만들 때 직접 얻은 정보만을 리용하는것이다. 이것은 경로조종오유를 없앨뿐아니라 수렴시간을 거의 0으로 떨군다. 그림 3-7의 망이 련결상태경로조종규약에 의하여 갱신되였다고 가정하고 경로기 A를 동작시키고 무엇이 발생하였는가를 보기로 하자.

련결상태에서 망정보전파

경로기 A가 동작할 때 그것은 hello라고 부르는 한가지 형태의 RIP파케트를 보낸다. hello파케트는 《여러분, 안녕하십니까? 나는 이 망에 새로 온 경로기입니다. 거기 누군가 있습니까?》라고 말하는것과 같다. 이 파케트는 그의 두 포구로 전송되며 경로기 B와 C가 그에 응답할것이다.

경로기 A가 경로기 B와 C로부터의 응답을 받으면 그는 련결상태규약 (LSP)프레임을 만들고 그것을 경로기 B와 C에로 전송한다. LSP프레임은 다음의 정보를 포함하는 경로보존프레임이다.

- 그 경로기의 이름 또는 식별자
- 그것이 붙어 있는 망들
- 매개 망에로 가는 도약수 또는 비용
- 그것의 hello프레임에 응답한 매개 망우의 다른 경로기들

경로기 B와 C는 경로기 A의 LSP프레임의 복사판을 만들어 그것을 그대로 망을 통하여 전송한다. 그러면 경로기 A의 LSP프레임을 받은 매 경로기는 매개 다른 경로기의 LSP프레임의 복사판을 유지한다. 경로기는 망을 도식화하고 경로조종표를 만드는데 이 정보를 리용할수 있다. 매 LSP프레임은 그것을 보낸 매개 경로기의 국부적인 경로정보만을 가지고 있으므로 이 망지도는 엄밀하게 직접정보로부터 만들어 진다. 하나의 경로기는 자기의 망그림이 완성될 때까지 LSP토막들을 맞추어 나간다.

경로기 A는 다음에 경로기 B 또는 C로부터의 LSP프레임요청을 만든다. LSP프레임요청은 그 경로기가 모든 알려 진 LSP프레임들의 복사를 전송할것을 요청하는 하나의 질문이다. 매개 경로기는 모든 LSP프레임들의 복사판을 가지고 있으므로 어느 한 경로기는 망에 있는 매 경로기로부터의 복사를 제공할수 있다. 이것은 경로기 A가 이 정보를 매 경로기들로부터 개별적으로 요청하지 않아도 되게 함으로써 통신의 대역너비를 절약하게 한다. 일단 LSP망이 돌아 가기 시작하면 갱신내용들은 두 시간에 한번씩 또는 변화가(어떤 경로기가 고장났는가 등) 발생하였을 때에만 전송된다.

련결상태방법에서 수렴시간

련결상태망이 가동하기 시작하였다. 경로기 B와 C는 자기들의 경로조종표를 다시 계산하지 않아도 된다. 그들은 그저 경로기 A로부터의 새로운 토막들을 더하고 통신량을 계속 통과시키면 된다. 이것이 수렴시간이 거의 0이라는것의 리유이다. 다만 매 경로기에 요구되는 변화는 새로운 토막들을 자기의 표에 첨가하는것이다. 거리벡토르법과는 달리 경로조종표를 표준화하기 위한 갱신은 요구되지 않는다. 경로기 B는 경로기 C를 통하여 어떤 망이 준비되여 있는가를 알리는 경로기 A로부터의 두번째 파케트를 필요로 하지 않는다. 경로기 B는 그저 경로기 A의 LSP정보를 그의 현존표에 첨가하며 이미 그 련결에 대하여 알고 있다.

련결상태환경에서 경로기고장으로부터의 회복

하나의 경로기가 떨어 져 나갔을 때 련결상태경로조종이 어떻게 반응하는가를 보기 위하여 그림 3-9를 다시 고찰하자. 이 실례의 목적을 위하여 경로조종규약이 거리벡토르법으로부터 련결상태법으로 갱신되였다고 가정하자. 또한 경로조종표들이 만들어 졌고 통신량은 정상으로 통과하고 있다고 가정하자.

만일 경로기 C가 정지된다면 그는 하나의 보존프레임(마지막숨이라고 하는)을 경로기 B에 전송하여 자기가 떨어 져 나간다는것을 알린다. 그러면 경로기 B는 가지고 있던 경로기 C의 LSP프레임의 복사판을 지우고 이 정보를 경로기 A에 전송한다. 이 두 경로기는 지금 새로운 망배치의 정당한 복사판을 가지고 있으며 망 4에로는 도달할수 없다는 것을 알고 있다. 만일 경로기 C가 살아 나지 못하고 아주 죽는다면 경로기 B가 경로기 C가 더는 자기가 보낸 파케트들에 응답하지 못한다는것을 알기까지에는 짧은 지연이 생긴다. 이 점에서 경로기 B는 경로기 C가 떨어 져 나갔다는것을 알게 될것이다. 다음에 그는 경로기 C의 LSP프레임을 자기의 표에서 지우며 경로기 A에 이 변화를 전송한다. 이리하여 두 체계는 새로운 망배치의 정당한 복사판을 가지게 된다.

여기서는 엄밀히 직접정보만을 취급하고 있으므로 거리벡토르법에서와 같은 무한대셈세기문제는 생기지 않는다. 우리의 경로기표들은 정확하고 망은 최소갱신량으로 기능하고 있다. 이것은 련결상태법을 많은 수의 망토막들에도 쓸수 있게 한다. 최대도약수는 127이지만 실제적인 정황에 따라 더 적을수도 있다.

련결상태경로조종에서의 보안

대부분의 련결상태경로조종규약들은 동적경로갱신이 원천에 대하여 어떤 준위의 인증을 지원한다. 이 기능을 거리벡토르법과 결합하는것도 불가능하지는 않지만 대부분의 거리벡토르규약들은 경로조종표갱신을 인증할 필요성을 느끼지 못하였다. 인증은 매 경로기가 믿음직한 호스트로부터의 경로조종표갱신만을 접수하도록 담보하는 훌륭한 수단으로 된다. 인증은 100% 안전하지는 못하지만 그것은 믿을수 있는 매 호스트로부터의 하나의 알림이다.

실례로 OSPF는 두가지 준위의 인증 즉 통과암호와 통보문요약(digest)이다. 통과암호인증은 경로표정보를 교환하는 매 경로기가 통과암호를 가질것을 요구한다. 하나의 경로기가 다른 경로기에로 OSPF경로정보를 보내려고 할 때 그것은 통과암호렬을 확인으로

포함한다. OSPF를 리용하는 경로기는 전송에 통과암호렬이 포함되여 있지 않으면 경로표갱신을 접수하지 않는다. 이것은 표갱신이 믿을수 있는 호스트로부터만 접수되도록 담보하는데 도움이 된다. 이 인증방법의 결함은 통과암호가 평문으로 전송된다는것이다. 이것은 망분석기를 가지고 망을 감시하고 있는 한 공격자가 OSPF표갱신들을 잡고 통과암호를 발견할수 있다는것을 의미한다. 통과암호를 아는 공격자는 그것을 리용하여 믿음성 있는 OSPF경로기로 가장하고 가짜경로정보들을 전송할수 있다.

통보문요약은 그것이 통과암호정보를 유선으로 교환하지 않는다는 점에서 보다 안전하다. 매개 OSPF경로기는 통과암호와 열쇠-식별자를 가지고 있다. OSPF표갱신을 전송하기전에 경로기는 일의적인 통보문요약을 생성하기 위한 알고리듬을 리용하여 OSPF표정보, 통과암호, 열쇠-식별자를 처리하여 이것들을 파케트의 뒤에 붙인다. 통보문요약은 표를 전송하는 경로기를 믿을수 있는 호스트로 간주할수 있는 암호화된 확인방법을 제공한다. 목적지경로기가 그 전송을 받을 때 그는 통과암호와 열쇠-식별자를 리용한다. 통보문이 인증되면 경로조종표갱신이 접수된다.

일러두기

OSPF에서 리용된 암호를 깨는것은 가능하지만 그렇게 하는데는 시간이 걸리고 처리능력이 소비된다. 이로 하여 통보문요약을 가지는 OSPF는 동적경로정보를 갱신하기 위한 훌륭한 선택으로 된다.

접속 및 무접속형통신

지금 체계들은 같은 론리적망에 위치하고 있는가에 관계없이 점 A로부터 점 B에로 정보를 전송할수 있다. 이제 다음의 문제가 제기된다. 《일단 우리가 목적을 이루면 어떻게 적당한 대화를 계속할것인가?》, 이것은 전송층에 관한 문제이다.

전송층은 우리가 통신례법의 규칙들을 설정하기 시작하는 곳이다. 한 체계로부터 다른 체계에로 정보를 넘기는것으로는 불충분하다. 또한 두 체계가 같은 수준의 례법으로 동작하도록 보장하여야 한다.

망통신례법에는 다음의 두가지 형태가 있다.

- 접속형통신
- 무접속형통신

접속형통신

접속형통신은 자료를 전송하기에 앞서 련결신호(handshake)라고 하는 조종정보들을 교환한다. 전송층은 련결신호를 리용하여 목적지체계가 정보를 수신할 준비를 갖추도록 보장한다. 접속형교환은 또한 자료가 원래의 순서로 송신되고 수신되도록 담보한다.

모뎀들은 어떤 정보를 보내기에 앞서 접속속도를 협상하여야 하므로 접속형통신의 사용자들이라고 볼수 있다. 망에서 이 기능은 IP나 AppleTalk에서 기발이라고 부르는 전

송층마당의 리용을 통하여 실현된다. IPX에서는 련결조종마당이라고 부른다. IP가 경로조종규약의 기초라면 TCP는 접속형통신을 만드는데 리용된다. IPX는 SPX를 리용하고 AppleTalk는 ATP를 리용하여 이 기능을 제공한다. 통신대화가 시작될 때 응용층(반드시 당신이 리용하는 프로그람은 아니라도)은 접속형규약이 필요한가를 결정한다.

Telnet는 이러한 한가지 응용프로그람이다. Telnet대화가 시작될 때 응용층은 련결의 믿음성을 더잘 담보하기 위하여 그것의 전송봉사로서 TCP를 요구한다. 련결신호가 어떻게 동작하는가를 보기 위하여 이 대화가 어떻게 확립되는가를 고찰하자.

TCP 3 -파케트련결신호

콤퓨터에서 원격접속을 설정하기 위하여 Telnet thor.foobar.com이라고 건반입력한다고 하자. 이 요청이 전송층을 통과할 때 두 체계를 련결하는데 TCP가 선택되여 접속형통신이 확립될수 있다. 전송층은 동기화기발(SYN)을 1로 설정하고 다른 모든 기발들은 0으로 설정한다. IP는 여러개의 기발마당을 리용하되 2진체계를 리용하여 값들을 설정한다.

SYN을 1로 설정하고 다른 마당들은 모두 0으로 설정하면 다른쪽의 체계는 (thor.foobar.com) 우리가 그 체계와 새로운 통신대화를 설정하려고 한다는것을 알게 된다. 이 요청이 다음에 나머지 층들을 통과하고 원격체계에 도착하여 그쪽의 OSI층들을 따라 올라 가게 된다.

원격체계에 봉사가 준비되여 있다면 이 요청은 접수되고 응답되는데 전송층에 도착할 때까지 그 탄창을 따라 전송된다. 전송층은 원래의 체계가 그러했던것처럼 SYN기발을 1로 설정하고 응답기발(ACK)도 1로 설정한다. 이것은 원래의 체계에 자기의 전송이 수신되였으며 자료전송이 OK이라는것을 알게 한다. 이 요청은 탄창을 통과하여 선을 따라 원래의 체계에로 전송된다.

원래의 체계는 다음에 SYN기발을 0으로 하고 ACK기발은 1로 하여 이 프레임을 Thor에 도로 전송한다. 이것은 Thor에게 《나는 당신의 응답에 답례를 보내며 자료를 보내려고 한다.》라는것을 알리는것이다. 이 점에서 자료가 전송되게 하며 매개 체계는 자기가 수신한 매 파케트에 대하여 하나의 답례를 전송하여야 한다.

No.	Siz	Source	Destination	Layer	Summary
1	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1042 --> TELNET SYN
2	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:TELNET --> 1042 ACK SYN
3	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1042 --> TELNET ACK
4	82	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Cmd=Do; Code=Suppress Go Ahead; Cmd=Will; Code=Termin
5	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:TELNET --> 1042 ACK
6	70	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Cmd=Do; Code=Terminal Type; Cmd=Do; Code=Terminal Spe
7	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Cmd=Won't; Code=; Cmd=Will; Code=Terminal Type;
8	73	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Cmd=Will; Code=Suppress Go Ahead; Cmd=Do; Code=; Cmd=
9	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:TELNET --> 1042 ACK
10	67	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Cmd=Subnegotiation Begin; Code=; Data=.P...
11	76	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Cmd=Subnegotiation Begin; Code=Terminal Speed; Data= ....
12	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1042 --> TELNET ACK
13	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:TELNET --> 1042 ACK
14	92	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Cmd=Subnegotiation Begin; Code=Terminal Speed; Data= .38
15	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Cmd=Do; Code=Echo;
16	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Cmd=Won't; Code=Echo;
17	129	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Cmd=Will; Code=Echo; Data= .Red Hat Linux release 4.1 (Va
18	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Cmd=Do; Code=Echo;
19	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:TELNET --> 1042 ACK
20	65	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=login:
21	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1042 --> TELNET ACK

그림 3-10. 접속형통신의 한가지 실례

그림 3-10은 Loki라는 체계로부터 Thor라는 체계에로의 하나의 telnet대화를 보여 준다. 매행은 한 체계로부터 다른 체계에로 전송된 하나의 프레임을 표현한다. 원천 및 목적지체계가 제시되여 있고 그 프레임에 대한 개요정보가 제시되여 있다. 첫 3개의 프레임은 telnet가 아니라 TCP프레임이며 이것들은 우에서 설명된 련결을 수행한다. TCP가 일단 련결을 설정하면 telnet는 요구되는 자료전송에 착수할수 있다. 대화에서 뒤에 나타나는 TCP프레임들은 답례를 위한것들이다. 언급된바와 같이 접속형규약에서는 매 프레임에 대하여 답례를 보내야 한다. 프레임이 만일 정보를 위한 요청이였다면 응답은 요청된 정보를 전송하는 형태일수 있다. 그러나 만일 응답을 요구하지 않는 프레임이 보내졌다면 목적지체계는 그 프레임이 수신되였다는 답례를 보내야 한다.

아직 련결신호와 접속형통신에 대하여 애매한것이 있다면 한가지 비유를 보기로 하자. 한 사람이 친구를 찾아서 그에게 토요일 밤에 망모임이 있으니 자기의 콤퓨터로 참가할것을 알리려고 한다고 하자. 그는 다음의 절차로 움직인다.

- 친구의 전화번호를 돌린다(SYN=1, ACK=0).
- 친구가 전화를 들고 말한다. 《여보시오.》(SYN=1, ACK=1)
- 그가 대답한다. 《안녕한가, F. 나는 D요.》(SYN=0, ACK=1)

그는 다음에 모임에 대한 자료를 전송하기 시작한다. 그가 잠간 중지할 때마다 F는 어떤 정보를 전송하든지(《예, 토요일 저녁에 시간이 있습니다.》등) 또는 자기가 수화기를 놓지 않았다는것을 알리기 위한 응답신호(ACK)를 어떤 형태로 보낼것이다.

대화가 끝나면 그는 《안녕히》라고 하고 련결을 끊게 되는데 이것은 서로 대화가 끝나고 전화를 끊어도 된다는것을 알리기 위한 련결신호이다. 전화를 놓으면 이 접속형통신대화는 완성된다.

접속형통신의 목적은 간단하다. 이것은 아래층들이 덜 안정하다고 간주될수 있을 때 믿음성 있는 통신대화를 제공한다. 전송층에서 믿음성 있는 련결성을 보장하는것은 자료가 손실될수 있을 때 통신의 속도를 높이는데 도움이 된다. 이것은 재전송프레임이 만들어 지고 전송되기전에는 그 자료가 응용층까지의 모든 경로를 통과하지 못하기때문이다. 이것은 적은 량의 잡음이나 횡단선에 의하여 통신대화가 죽을수 있는 모뎀통신에서 중요하지만 망에 기초한 통신에서보다는 유용하지 못하다.

무접속형통신

무접속형규약에서는 매 파케트에 대하여 초기의 련결신호나 답례를 보낼것을 요구하지 않는다. 무접속형전송을 리용할 때 그것은 최선의 노력으로 자료를 전송하되 응용층답례와 같은 다른 층들의 안전성에 기초하여 자료가 믿음성 있게 전송된다는것을 담보한다. IP의 사용자데타그람규약(UDP)과 IPX의 NetWare핵심규약(NCP)은 무접속형전송의 실례들이다. 이 두 규약은 무접속형통신을 리용하여 경로정보와 봉사기정보를 전송한다. AppleTalk는 자료대화에서는 무접속형통신을 리용하지 않고 이름결합규약(NBP)을 가지는 봉사기를 공시할 때 이것을 리용한다. 방송들은 항상 무접속형전송을 리용하여 전송된다.

No.	Size	Source	Destination	Layer	Summary
1	198	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Lookup ???/games.tar.gz
2	174	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Lookup for games.tar.gz
3	182	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Get File Attributes for games.tar.gz
4	142	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Get File Attributes
5	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 0; 1024 bytes
6	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
7	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 1024; 1024 bytes
8	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
9	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 2048; 1024 bytes
10	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
11	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 3072; 1024 bytes
12	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
13	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 4096; 1024 bytes
14	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
15	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 5120; 1024 bytes
16	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
17	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 6144; 1024 bytes
18	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
19	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 7168; 1024 bytes
20	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
21	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 8192; 1024 bytes
22	1,170	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	nfs	Reply Read From File; 1024 bytes
23	194	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	nfs	Call Read From File games.tar.gz; Offset 9216; 1024 bytes

그림 3-11. NFS는 무접속형대화를 하는데 UDP를 리용한다.

무접속형통신의 한가지 실례로서 그림 3-11의 망파일체계(NFS)부분을 검사해 보자. NFS는 IP에서 파일공유를 가능하게 하는 봉사이다. 그것은 자기의 전송층규약으로서 UDP를 리용한다. 모든 자료답례는 추가정보에 대한 요청형태로 되여 있다는것을 알수 있다. 목적지체계(Thor)는 원천체계(Loki)가 추가정보를 요청하면 마지막파케트가 수신되였다고 가정한다. 반대로 만일 Loki가 Thor로부터 응답을 받지 못한다면 NFS는 그 정보를 다시 요청하게 된다. 만일 많은 재전송을 요구하지 않는 안정한 련결을 가지고 있다면 NFS가 오유수정을 하도록 하는것이 매우 효과적인 통신방법으로 된다. 왜냐하면 그것은 불필요한 답례를 하지 않기때문이다.

이러한 통신형태가 앞에서 본 접속형통신과 어떻게 다른가를 알기 위하여 또 하나의 비유를 보기로 하자. 이번에도 D가 F를 찾아서 토요일 저녁에 있는 망모임에 초청한다고 하자. D는 F의 번호를 돌리는데 이번에는 전화자동응답기로 찾는다. 그는 모임이 언제 열리며 무엇이 있어야 하는가 하는 상세한 통보를 거기에 남긴다.

F가 대답하던 첫번째 경우와 달리 D는 지금 다음의 내용들에 의거하고 있다.

- 이 번호가 F의것이라는것을 확인하지 못했어도 정확한 전화번호를 돌릴수 있는 자기의 능력
- 통신도중에 전화회사가 그의 전화련결을 끊지 않는다는 사실
- 자동전화응답기가 테프를 끊지 않고 통보문을 기록한다는것
- F의 고양이가 테프와 뼐을 분간하는 능력
- 전원고장이 없다는것(전원고장은 통보문을 잃게 할수 있다.)
- 지금과 모임날자사이의 기간에 F가 이 통보문을 볼것이라는것

알수 있는바와 같이 그는 친구가 그 통보문을 실례로 수신할것이라는 실제적인 확신을 못 가지고 있다. 그는 F가 그 통보를 적당한 시간에 볼수 있도록 할것을 전기회사나 전화자동응답기 등에 기대하고 있는것이다.

만일 그가 자료전송의 믿음성을 담보하려고 하였다면 그는 《목요일에 회답을 바

람》이라는 형태로 응용층답례요구를 보낼수 있을것이다. 만일 응답을 받지 못했다면 그 자료를 다시 전송할수 있다.

그러면 접속형통신과 무접속형통신중에 어느것이 더 리용하기 좋은 전송인가? 아쉽게도 그 대답은 응용층이 지적하는것이다. 만일 telnet가 TCP를 원한다면 그것이 UDP를 쓰도록 강요할수 없다.

보안문제

접속형통신의 기발마당을 잘 리용한 한가지 기술은 방화벽이다. 방화벽은 기발마당의 정보를 리용하여 련결이 내부의것인가, 외부의것인가를 결정하며 자기의 규칙표에 따라 그 련결을 허용 또는 거부한다.

실례로 방화벽규칙이 내부사용자는 인터네트로 접근할수 있도록 허용하고 외부사용자가 내부체계를 접근하는것을 막는다고 하자. 이것은 매우 일반적인 보안방책이다.

이것을 어떻게 실행할것인가

내부자료흐름들을 모두 막는것은 내부사용자들이 자기들의 자료요구에 대한 응답을 받는것을 항상 금지하는것으로 되므로 불가능하다. 들어 오는 응답들은 허용하면서 외부체계가 내부체계와의 련결을 설정하는것은 거부하는 어떤 방법이 필요하다. 이 비밀은 바로 TCP기발들에 있다.

TCP에 기초한 대화에서는 자료를 전송하기전에 련결신호가 필요하다는것을 알고 있다. 만일 SYN마당에는 1을 설정하고 다른 모든 마당들에는 0을 설정한 모든 들어 오는 프레임들을 막는다면 외부사용자가 내부체계와 하나의 련결을 설정하는것을 막을수 있을것이다. 이 설정들은 초기련결신호에서만 리용되고 전송의 다른 부분에서는 나타나지 않으므로 그것은 외부사용자를 막는 효과적인 방법으로 된다. 외부사용자가 내부체계에 련결할수 없으면 그들은 자료를 전송할수 없거나 또는 그 체계로부터 자료를 꺼내갈수 없다.

주 의

많은 방화벽들은 모든 UDP련결을 거부한다. UDP는 기발마당을 가지고 있지 않으며 대부분의 방화벽들은 자료가 련결요청인지, 응답인지를 결정하는 효과적인 방법을 가지고 있지 못하다. 이로 하여 동적파케트려과방화벽이 생겨 나고 널리 쓰이게 되였다. 이것들은 모든 련결대화들을 감시하고 기억한다. 동적파케트려과를 리용하면 외부호스트로부터 오는 UDP파케트를 그 호스트가 이전에 UDP를 리용하는 정보를 위하여 질문된적이 있을 때에만 허용하는 려과규칙을 만들수 있다. 이것은 들어오는 UDP응답들만이 방화벽을 통과하는것을 담보한다. 파케트려과 또는 어떤 대리방화벽들은 TCP련결에서만 효과적으로 동작하지만 동적파케트려과방화벽은 UDP도 안전하게 통과시킬수 있다.

망 봉 사

우리는 지금 두 원격체계가 같은 준위의 통신을 리용하고 있다는것을 확신할수 있다.

이제는 봉사기에게 우리가 무엇을 원하는가를 어떻게 알리겠는가? 콤퓨터는 1s에 수많은 요청을 처리할수 있는 강력한 도구이지만 《당신은 내가 무엇을 말하는지 아는가?》라는 물음에서는 아직 문제를 가지고 있다. 그러므로 우리가 무엇을 원하는가를 체계가 정확히 알도록 하는 방법이 있어야 한다.

무엇을 원하는가를 콤퓨터가 알도록 담보하기 위하여서는 대화층을 들여다 보아야 한다.

주 의

대화층에 대한 고찰로부터 그것이 봉사요구를 적당히 형식화하는데 책임이 있는 층이라는것을 알수 있을것이다.

봉사란 봉사기에서 돌아 가는 처리 또는 응용프로그람으로서 그것은 망사용자에게 어떤 리득을 제공한다. 전자우편은 가치 있는 봉사의 한가지 좋은 실례로 된다. 우편의 뢰기를 가지고 체계에 련결할 때 그 체계는 우편통보문들을 대기하고 있게 된다. 파일 및 인쇄기공유도 망봉사의 실례로 된다.

봉사는 특정의 포구 또는 소케트에 접속함으로써 호출된다. 포구는 체계에 있는 가상적인 우편홈으로 생각할수 있다. 개별적인 우편홈(포구번호)은 체계에서 돌아 가는 매 봉사 또는 응용프로그람들에 배당된다. 사용자가 하나의 봉사를 호출하려고 할 때 대화층은 그 요청이 정확한 우편홈 또는 포구번호에 도달하도록 담보할 책임을 진다.

UNIX 또는 NT체계에서 IP포구번호들이 하나의 파일로서 봉사들에 사상된다. 봉사파일들에 대한 간단한 내용을 표 3-6에 보여 준다. 첫렬은 봉사의 이름, 두번째 렬은 포구와 리용되는 전송이다. 세번째 렬은 그 봉사에 의하여 제공되는 간단한 기능서술이다. 표 3-6은 몇가지 IP봉사들에 대한 간단한 목록이다. 보다 많은 정보를 얻으려면 RFC1700을 참고하면 된다.

주 의

이 포구번호들은 UNIX에 관한것이 아니다. 실례로 SMTP를 리용하는 조작체계는 포구 25를 리용하여야 한다.

표 3-6에 요약된 파일들에 따르면 포구 23에서 수신된 TCP요청은 telnet대화인것으로 가정되며 원격접근을 취급하는 응용프로그람에 보내진다. 만일 요청된 포구가 25이면 우편봉사가 요청되여 그 대화는 우편프로그람에 보내진다.

표 3-6의 파일들은 인터네트데몬(inetd)이라고 하는 처리에 의하여 UNIX체계에서 리용된다. inetd는 UNIX체계의 매개 목록화된 포구들을 감시하며 그 포구에 봉사를 제공하는 응용프로그람을 촉발시켜 주는 책임을 지고 있다. 이것은 자주 호출되지 않는 포구들에 대하여 체계를 관리하는 한가지 효과적인 방법이다. 이 과정은 봉사가 실지로 필요할

때에만 운영되고 체계자원(기억, CPU시간 등)을 리용한다. 봉사가 끌나면 이 과정은 휴식상태로 들어 가서 inetd가 다시 호출되기를 기다린다.

표 3-6 간략화된 봉사파일

봉사이름	포구 및 전송	기 능
ftp-data	20/tcp	실제파일정보전송에 리용
ftp	21/tcp	대화지령전송에 리용
telnet	23/tcp	원격대화만들기
SMTP	25/tcp	전자우편배달
Whois	43/tcp	내부령역이름찾기
Domain	53/tcp	령역이름대기렬
Domain	53/udp	DNS지역전송
Bootps	67/udp	bootp봉사기
Bootpc	68/udp	boots의뢰기
POP3	110/tcp	우편국 V.3
nntp	119/tcp	망뉴스전송
Ntp	123/tcp	망시간규약
Ntp	123/udp	망시간규약
NetBIOS-ns	137/tcp	nbns
NetBIOS-ns	137/udp	nbns
NetBIOS-dgm	138/tcp	nbdgm
NetBios-dgm	138/udp	nbdgm
NetBIOS-ssn	139/tcp	nbssn
SNMP	161/udp	단순망관리규약
SNMP-trap	162/udp	단순망관리규약

자주 리용되는 응용프로그람들은 듣기방식으로 돌아 가고 있어야 한다. 실례로 Web봉사기접근은 보통 포구 80을 리용한다. 이것은 표 3-6의 봉사파일에서 inetd에 의하여 취급되는 과정으로 기입되여 있다. 이것은 Web봉사기가 하루에도 많은 요청들에 봉사하도록 호출되기때문이다. 페지요청이 있을 때마다 inetd를 기동시키는것보다는 이 과정이 모든 시간 계속 돌고 있도록 하는것이 보다 효과적이다.

이 모든 포구번호들을 잘 알려 진 포구라고 부른다. 잘 알려 진 포구들은 어느 포구가 그 봉사에서 쓰이는가를 알려고 할 필요없이 누구나 봉사를 호출하도록 담보하는데 사용되는 사실표준들이다. 실례로 포구 573이 그 어느 봉사에서도 리용되지 않고 있다는것을 알고 누구의 간섭도 없이 그 포구에 Web봉사기를 설치할수 있다. 이때 문제는 모든 사용자들이 그 봉사가 포구 80에 준비되였다고 알고 있으며 그것을 찾을수 없다는것이다. 그러나 때로는 포구들을 바꾸는 일도 생겨 날수 있다.

주 의

사실표준이란 규정이나 법에 의해서가 아니라 대중성에 의하여 결정되는 표준을 말한다.

포구 0 ~ 1023은 인터네트번호위임기구(IANA)에 의하여 가장 잘 알려 진 봉사들용으로 정의되였다. 포구들은 7200까지 지정되였으나 1024아래의 포구들이 인터네트통신에서 많이 쓰인다. 이 배당은 엄격한 규칙은 아니며 오히려 누구나가 같은 포구에서 공개적인 봉사를 제공하도록 담보하게 되여 있는것이다. 실례로 만일 Microsoft의 Web페지로 접근하려고 한다면 그 봉사가 포구 80에서 제공된다고 가정할수 있다. 왜냐하면 이것이 그 봉사에 대하여 잘 알려 진 포구이기때문이다.

체계가 정보를 요구할 때 그것은 접근하려는 포구를 지적할뿐아니라 요청된 정보를 돌려 줄 때 어느 포구를 리용하여야 한다는것도 지적하여야 한다. 이 과제를 위한 포구번호들은 1024로부터 65535까지에서 선택되며 웃포구번호라고 부른다.

이것이 어떻게 동작하는가를 보기 위하여 그림 3-10의 telnet대화를 다시 고찰하자. Loki가 Thor와 telnet대화를 설정하려고 할 때 이것은 Thor의 포구 23에 접근하여 수행될것이다(포구 23은 telnet를 위한 잘 알려 진 포구이다.). 만일 프레임번호 2를 본다면 Thor가 포구 1042로 답례(ACK)를 보내고 있다는것을 알수 있다. 그것은 Loki가 Thor에게 보낸 원래 프레임의 대화정보가 1042의 원천포구와 23의 목적지포구를 지적하고 있기때문이다. 목적지포구는 프레임이 가고 있는 곳이며(Thor의 포구 23) 원천지포구는 응답을 보낼 때 어느 포구가 리용되여야 하는가 하는것이다(Loki의 포구 1042). 포구 23은 잘 알려 진 봉사포구이며 포구 1042는 응답에 리용되는 웃포구번호이다.

웃응답포구들은 동작중에 지정된다. 포구들이 준비되였는가에 따라 지정되므로 체계가 정보요청할 때 그것을 어느 포구로 수신할것인가를 예측하는것은 거의 불가능하다. 이로하여 방화벽목적으로 리용된 파케트려과기들은 때로 1023우의 포구들이 응답을 받기 위하여 모든 시간 열려 있도록 부정확하게 설정한다.

이것은 잘 알려 진 포구가 아닌 한 포구가 어떻게 하나의 봉사를 제공하는데 리용될수 있는가에 대한 리유들중의 하나를 제공하는것으로 된다. 파케트려과가 자기의 체계에서 돌아 가는 Web봉사기에 대한 접근을 막는다는것을 알고 있는 사용자는 그 봉사를 8001과 같은 웃포구번호에 배당할수 있다. 련결이 포구 1023우에서 이루어 지므로 그것은 막히지 않는다. 그 결과로 내부Web싸이트를 금지하는 보안방책과 그 집행을 위한 파케트려과기가 있음에도 불구하고 이 사용자는 URL에 따라 포구번호(8001)를 쓰는 한 자기의 Web싸이트를 성과적으로 광고할수 있게 된다. 이 URL은 다음과 같이 쓸수 있다.

http://thor.foobar.com:8001

:8001은 Web열람기가 80대신에 포구 8001을 리용하여 그 봉사기로 접근하여야 한다는것을 지적한다. 대부분의 파케트려과기는 가입등록기능이 좋지 못하므로 《내부Web싸이트금지》라는 방책을 집행하는데 책임 있는 망관리자는 아마 우연히 마주치지 않는 한 그것이 존재한다는것을 결코 알수 없을것이다.

일러두기

당신의 책임자가 Web을 돌아 다니면서 시간을 랑비한다고 당신을 추궁한다면 다음과 같이 말하는것이 좋다. 《나는 우리의 보안방책에 맞지 않는 배신적인 내부싸이트들에로의 련결을 추적하여 보안검열을 수행하고 있다. 이 사업은 우리의 방화벽체계가 불충분하기때문에 제기된다.》 만일 당신이 그 자리에서 파면 당하지 않는다면 그 사건이 책임자의 머리속에서 잊혀 지기전에 빨리 새로운 방화벽을 구입하자고 제기하면 된다.

No.	Source	Destination	Layer	Summary	Size	Interpacket	Absolute Time
1	Loki	Thor	tcp	Port:1051 --> SMTP SYN	64	8 µs	9:40:09 AM
2	Thor	Loki	tcp	Port:SMTP --> 1051 ACK SYN	64	968 µs	9:40:09 AM
3	Loki	Thor	tcp	Port:1051 --> SMTP ACK	64	857 µs	9:40:09 AM
4	Thor	Loki	tcp	Port:SMTP --> 1051 ACK PUSH	138	100 ms	9:40:10 AM
5	Loki	Thor	tcp	Port:1051 --> SMTP ACK	64	12 ms	9:40:10 AM
6	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	80	9 s	9:40:19 AM
7	Thor	Loki	tcp	Port:SMTP --> 1051 ACK PUSH	134	1 ms	9:40:19 AM
8	Loki	Thor	tcp	Port:1051 --> SMTP ACK	64	17 ms	9:40:19 AM
9	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	91	18 s	9:40:36 AM
10	Thor	Loki	tcp	Port:SMTP --> 1051 ACK	64	19 ms	9:40:36 AM
11	Thor	Loki	tcp	Port:SMTP --> 1051 ACK PUSH	97	9 ms	9:40:36 AM
12	Loki	Thor	tcp	Port:1051 --> SMTP ACK	64	28 ms	9:40:36 AM
15	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	93	21 s	9:40:57 AM
16	Thor	Loki	tcp	Port:SMTP --> 1051 ACK	64	11 ms	9:40:57 AM
17	Thor	Loki	tcp	Port:SMTP --> 1051 ACK PUSH	104	300 ms	9:40:57 AM
18	Loki	Thor	tcp	Port:1051 --> SMTP ACK	64	15 ms	9:40:57 AM
19	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	64	2 s	9:41:00 AM
20	Thor	Loki	tcp	Port:SMTP --> 1051 ACK PUSH	108	2 ms	9:41:00 AM
21	Loki	Thor	tcp	Port:1051 --> SMTP ACK	64	17 ms	9:41:00 AM
22	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	80	12 s	9:41:12 AM
23	Thor	Loki	tcp	Port:SMTP --> 1051 ACK	64	12 ms	9:41:12 AM
24	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	122	28 s	9:41:40 AM
25	Thor	Loki	tcp	Port:SMTP --> 1051 ACK	64	15 ms	9:41:40 AM
26	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	68	5 s	9:41:45 AM
27	Thor	Loki	tcp	Port:SMTP --> 1051 ACK	64	16 ms	9:41:45 AM
28	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	64	6 s	9:41:50 AM
29	Thor	Loki	tcp	Port:SMTP --> 1051 ACK	64	17 ms	9:41:50 AM
30	Thor	Loki	tcp	Port:SMTP --> 1051 ACK PUSH	102	275 ms	9:41:51 AM
31	Loki	Thor	tcp	Port:1051 --> SMTP ACK	64	18 ms	9:41:51 AM
32	Loki	Thor	tcp	Port:1051 --> SMTP ACK PUSH	64	3 s	9:41:53 AM
33	Thor	Loki	tcp	Port:SMTP --> 1051 ACK PUSH	98	2 ms	9:41:53 AM
34	Thor	Loki	tcp	Port:SMTP --> 1051 ACK FIN	64	960 µs	9:41:53 AM

그림 3-12. 이것이 표준우편전송처럼 보이지만 그것은 사실상
목적지체계에로의 한 우편통보문을 가짜로 만드는것이다.

포구번호를 바꾸는 문제를 보기 위하여 그림 3-12에서 그 대화를 찾아 보자. 그 대화가 단순우편전송규약(SMTP)이므로 그것은 사실상 포구 25(SMTP를 위한 잘 알려 진 포구)에 지적된 telnet대화이다. 우리는 이 대화를 기록하는 분석기를 속여서 우리가 그저 다른데로 우편을 전송하는 하나의 우편체계를 가지고 있다고 생각하게 하였다. 대부분의 방화벽들은 진행중의 대화를 식별하기 위하여 목적지포구를 리용하므로 같은 방식으로 속게 될것이다. 그들은 동반되는 실제적인 응용프로그람을 보지 않는다. 이러한 활동형식은 누군가를 속이는것 또는 우편통보문을 위조하는것과 류사하다. 일단 내가 원격우편체계에 련결되였다면 나는 어디선가 오는 통보문인것처럼 가장할수 있다. 우편머리부에 있는 경로정보가 검사되지 않는 한(사용자에게 친절한 대부분의 우편프로그람들은 이 정보를 그저 버린다.) 이 정보의 실제적인 원점은 추적될수 없다.

이러한 기만행위때문에 침입검출체계(IDS)가 생겨 나고 퍼지게 되였는데 이 체계는 이러한 형태의 활동들을 잡도록 프로그람화되였다. 그림 3-12를 다시 보고 이번에는 전송체계가 리용한 프레임크기를 검사해 보자. 전송된 가장 큰 프레임은 122byte이다. 이것은 telnet대화임을 가리킨다. 그것은 telnet가 타자된 매 문자에 대하여 답례할것을 요구하기때문이다. 이것이 자료를 전송하는 실제적인 우편체계였다면 우리는

1500byte에 가까운 파케트크기를 보았을것이다. 그것은 SMTP는 하나의 문자가 하나의 프레임으로 전송될것을 요구하지 않기때문이다. 좋은 IDS는 이러한 불일치를 찾아 내도록 조정될수 있다.

그림 3-13은 이 거짓대화의 마지막출구를 보여 준다. 머리부정보없이 이 통보문이 bgates@microsoft.com로부터 왔다는것을 믿을수 있다. 그 통보문이 Microsoft령역안의 우편체계에 의하여 접촉되지 않았다는것은 그것이 가짜라는것을 의미한다. 이것은 이전에 인터네트의 보안문제를 강의할 때 리용된 실례이다. 읽은것 특히 그것이 인터네트로부터 읽은것이라면 다 믿지는 말아야 한다.

```
From bgates@microsoft.com  Wed Feb  5 16:42:21 1997
Return-Path: <bgates@microsoft.com>
Received: from loki.foobar.com (loki.foobar.com [10.2.2.20])
          by thor.foobar.com (8.8.4/8.8.4) with SMTP
        id QAA00887 for cbrenton@thor.foobar.com; Wed, 5 Feb 1997 16:41:04 -0500
Date: Wed, 5 Feb 1997 16:41:04 -0500
From: bgates@microsoft.com (Bill Gates)
Message-Id: <199702052141.QAA00887@thor.foobar.com>
Subject: Quake Party
Status: R

The party sounds cool! I'll bring the P5's and the cheeze wiz!

Later...
```

그림 3-13. 거짓우편통보문의 출력

체계들사이의 류사한 대화들을 구별하는데 포구번호들이 리용될수도 있다. 실례로 그림 3-10을 보자. 여기서는 이미 Loki로부터 Thor에게로 가는 하나의 telnet대화를 가지고 있다. 만일 4개 또는 5개의 대화들이 만들어 진다면 어떤 일이 생길것인가? 모든 대화들은 다음의 정보들을 공통적으로 가진다.

원천IP주소 : 10.2.2.20(loki:foobar.com)
목적지IP주소 : 10.2.2.10(thor.foobar.com)
목적지포구 : 23(telnet용으로 잘 알려 진 포구)

원천포구들은 매 개별적인 대화를 식별하는데 리용될수 있는 유일한 구별정보이다.

첫 련결은 이미 자기의 련결을 위하여 원천포구를 1042로 지적하였다. 그후에 설정되는 매개 련속적인 telnet대화는 그것을 유일하게 식별하기 위하여 어떤 다른 웃포구번호로 지정될것이다. 지정된 실제적인 번호는 원천체계에서 현재 무엇이 리용되지 않고 있는가에 기초하고 있을것이다. 실례로 포구 1118, 1398, 4023 그리고 6025들이 다음번 4개의 대화를 위하여 원천포구로써 리용될수 있다.

실제적인 응답포구번호는 사실상 문제로 되지 않는다. 그것은 어쨌든간에 두 체계사이의 특정대화를 유일하게 식별할수 있다. 만일 우리가 동시에 발생하는 많은 대화들을 감시하고 있었다면 그 결과는 그림 3-14와 류사하게 보일것이다. 매개 대화를 식별하는데 지금 여러개의 응답포구들이 리용되고 있다.

No.	Source	Destination	Layer	Summary	Size
1	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=l	64
2	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=l	64
3	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1036 --> TELNET ACK	64
4	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=s	64
5	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=s	64
6	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1036 --> TELNET ACK	64
7	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=.	64
8	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=.	64
9	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1036 --> TELNET ACK	64
10	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=install.log.	71
11	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1036 --> TELNET ACK	64
12	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=[cbrenton@thor /tmp]$	80
13	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1036 --> TELNET ACK	64
14	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=l	64
15	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=l	64
16	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> TELNET ACK	64
17	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=s	64
18	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=s	64
19	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> TELNET ACK	64
20	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=.	64
21	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=.	64
22	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> TELNET ACK	64
23	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=install.log.	71
24	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> TELNET ACK	64
25	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=[cbrenton@thor /tmp]$	80
26	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> TELNET ACK	64
27	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=l	64
28	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=l	64
29	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1039 --> TELNET ACK	64
30	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	telnt	Data=s	64
31	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	telnt	Data=s	64
32	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1039 --> TELNET ACK	64

그림 3-14. Loki와 Thor사이에서 진행되는 여러개의 telnet대화

IP는 포구들을 리용하는 유일한 규약은 아니다. AppleTalk와 IPX도 포구들을 리용하는데 그것을 소케트라고 부른다. 서로 다른 포구들을 식별하는데 10진수를 쓰는 IP나 AT와 달리 IPX는 16진수를 사용한다. AppleTalk와 IPX에서도 잘 알려 진 포구와 웃포구들은 IP때와 같이 기능한다. AppleTalk와 IPX는 그리 많이 쓰이지 않는다.

파일전송규약(FTP): 특수경우

지금까지 본 모든 실례들에서 원천체계는 특정봉사로 접근할 때 목적지체계에로의 하나의 봉사련결을 만든다. 여러 사용자가 이 봉사를 요구하지 않는 한 하나의 련결대화만이 요구된다.

FTP는 한 체계로부터 다른 체계에로 파일정보를 전송하는데 쓰인다. FTP는 전송층으로서 TCP를 리용하며 통신을 위하여 포구 20과 21을 쓴다. 포구 21은 대화정보(사용자이름, 통과암호, 지령들)를 전송하는데 쓰이며 포구 20은 자료포구라고 하는데 실제적인 파일을 전송을 하는데 쓰인다.

그림 3-15는 두 체계(Loki가 Thor에게 련결하고 있다.)사이의 FTP지령대화를 보여준다. 대화의 시작에 있는 3-파케트TCP련결신호를 주목하시오. 이것은 이 장의 앞에서 접속형통신을 고찰할 때 서술되였다. 모든 통신들은 목적지포구로 21을 리용하고 있는데 이것을 간단히 FTP포구라고 부른다. 포구 1038은 Loki가 응답을 받을 때 리용한 우연적으로 정해 진 웃포구이다. 이 련결은 포구 1038에서 Loki에 의하여 포구 21의 Thor에게로 시작되였다.

No.	Size	Source	Destination	Layer	Summary
1	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> FTP SYN
2	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP --> 1038 ACK SYN
3	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> FTP ACK
4	164	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[Service ready for new user.]
5	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> FTP ACK
6	73	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	ftp	Command=USER(User Name)
7	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP --> 1038 ACK
8	95	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[User name okay, need password.]
9	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> FTP ACK
10	71	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	ftp	Command=PASS(Password)
11	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP --> 1038 ACK
12	88	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[User logged in, proceed.]
13	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	ftp	Command=SYST(System Operating System Type)
14	77	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[Name system type.]
15	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> FTP ACK
17	66	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	ftp	Command=TYPE(Representation Type)
18	78	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[Command okay.]
19	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1038 --> FTP ACK

그림 3−15. 두 체계사이의 FTP지령대화

그림 3−16은 Loki가 Thor로부터의 파일전송을 시작하고 있다는것을 보여 준다. 행 7, 8 그리고 9는 TCP 3−파케트련결신호를 보여 준다. 10으로부터 24까지의 행은 실제적인 자료전송을 보여 준다.

이것은 좀 이상한 점을 가지고 있다. Loki와 Thor는 그림 3−15에서 본것처럼 아직 포구 1038과 21우에서 적극적인 대화를 하고 있다. 그림 3−16은 그림 3−15에서 보여 준 것과 병렬로 진행되는 두번째의 개별적인 대화이다. 이 두번째 대화는 실제적인 파일 또는 자료를 전송하기 위하여 시작된다.

No.	Size	Source	Destination	Layer	Summary
2	66	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	ftp	Command=TYPE(Representation Type)
3	78	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[Command okay.]
4	79	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	ftp	Command=PORT(Data Port)
5	88	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[Command okay.]
6	77	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	ftp	Command=RETR(Retrieve File)
7	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 SYN
8	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1037 --> FTP-DATA ACK SYN
9	64	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
10	132	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	ftp	Reply:[File status okay; about to open data connection.]
11	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
12	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
13	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1037 --> FTP-DATA ACK
14	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
15	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
16	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
17	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1037 --> FTP-DATA ACK
18	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1034 --> FTP ACK
19	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK PUSH
20	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
21	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
22	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK
23	64	LOKI.FOOBAR.COM	THOR.FOOBAR.COM	tcp	Port:1037 --> FTP-DATA ACK
24	1,518	THOR.FOOBAR.COM	LOKI.FOOBAR.COM	tcp	Port:FTP-DATA --> 1037 ACK

그림 3−16. FTP자료대화

이 련결에 대하여 좀 이상한것이 있다. 행번호 7을 자세히 보시오. Loki가 아니라 Thor가 실례로 파일정보를 전송하기 위하여 TCP 3−파케트련결신호를 시작하고 있다. Loki는 포구 21로 원래의 FTP지령대화를 시작할 책임이 있지만 Thor는 실제적으로 FTP 자료대화를 시작하고 있는것이다.

이것은 인터네트에로의 FTP대화를 지원하기 위하여서는 포구 20의 인터네트호스트로부터 내부망에로의 련결이 확립되도록 허용하여야 한다는것을 의미한다. 만일 우리의

방화벽장치가 내부로의 자료흐름을 위한 원천포구를 정의할수 없게 한다면 1023우의 모든 포구들을 완전히 열어 놓아야 한다. 이것은 정확히 말하여 가장 안전한 보안자세로는 되지 못한다.

피동 FTP

피동FTP라고 부르는(PASV FTP) FTP전송의 두번째 형식도 있다. 피동FTP는 포구 21을 통하여 지령을 보낸다는 점에서는 표준FTP와 같다. 피동FTP와 표준FTP사이의 차이는 어떻게 자료대화가 시작되는가 하는데 있다. 피동FTP는 대부분의 Web열람기들에서 지원하는 방식이다.

자료를 전송하기전에 의뢰기는 PASV방식의 전송을 요청할수 있다. 만일 FTP봉사기가 이 요청에 답례한다면 의뢰기는 봉사기대신에 TCP 3-파케트련결신호를 시작할수 있게 허가된다. 그림 3-17은 피동FTP를 리용하는 두 체계를 보여 준다. 파케트 21은 《이콤퓨터》(또는 FTP의뢰기)가 PASV FTP를 요청하고 있는것을 보여 준다. 파케트 22에서 FTP봉사기가 응답하여 PASV방식이 시작된다는것을 알린다.

그림 3-17. 피동방식의 FTP대화

파케트 23에서 무엇이 일어 나는가를 보자. FTP의뢰기는 자료를 전송하기 위하여 TCP3-파케트련결신호를 시작한다. 이것은 한 문제를 해결하지만 또 다른 문제가 생기게 한다. 의뢰기가 그 대화를 시작하기때문에 우리는 지금 포구 20으로부터 들어 오는 접근을 막을수 있다. 이것은 내부로의 보안방책을 좀 엄격히 하게 한다. 그러나 이 피동대화를 시작하기 위하여 의뢰기는 원천과 목적지용으로 우연적인 웃포구번호를 사용하고 있다는데 주목하여야 한다. 이것은 PASV FTP를 지원하기 위하여서는 바깥쪽으로의 대화는 모두 1023우의 포구들에서 설정되게 하여야 한다는것을 의미한다. 만일 바깥쪽으로의 인터네트접근을 조종하려고 하는것은 그리 좋은 보안자세가 아니다(인터네트게임을 금지하는것과 같다.).

관리자들이 방화벽이나 망주소변환장치(NAT)를 리용할 때 또 하나의 문제가 생길 수 있다. 그 문제는 FTP가 두개의 분리된 대화를 사용한다는 사실을 기본내용으로 하고 있다.

주 의

NAT는 IP주소를 사설번호로부터 법적번호로 변환할수 있게 한다. 이것은 자기 망에서 사용하고 있는 IP주소가 ISP에 의하여 배당된것이 아닐 때 유용하다. NAT에 대하여서는 제5장의 방화벽을 론의할 때 더 보기로 한다.

인터네트상에서 큰 파일 하나를(Microsoft로부터의 60MB짜리 최신접속파일이라고 하자.) 전송하고 있는 동안 포구 20에로의 조종대화는 조용하다. 이 대화는 파일을 전송하는 동안 그 전송이 끝날 때까지 아무 정보도 전송하지 않아도 된다. 일단 그것이 끝나면 체계는 그 파일이 그대로 수신되였다는것을 조종대화를 통하여 답례한다.

그 파일을 전송하는데 많은 시간이 걸렸다면(약 한시간이상) 방화벽 또는 NAT장치는 그 조종대화가 더는 정상이 아니라고 가정할수 있다. 그 장치는 두 체계사이에서 오래동안 자료전송을 보지 못하였으므로 련결이 끊어 졌다고 가정하고 자기의 표에서 그 대화항목을 지워 버린다. 이것은 잘못된것이다. 일단 파일전송이 끝나면 체계는 그 파일이 수신되였다는것을 담보하기 위한 련결신호에 의미를 가지지 않는다. 이 문제의 대표적인 증세는 파일을 전송 또는 수신하는 의뢰기가 99%는 련결되여 있다는것이다.

다행히도 대부분의 제작자들은 이 시간한계설정을 조절할수 있게 하고 있다. 만일 이러한 증상을 경험하고 있다면 자기의 방화벽 또는 NAT장치를 검사하여 그것이 TCP시간한계설정을 가지고 있는가를 알아 보는것이 좋다. 만일 그렇다면 간단히 그 값을 증가시키면 된다. 대부분의 체계들은 시간한계값을 한시간으로 정하고 있다.

다른 IP봉사

많은 응용프로그람봉사들은 IP를 리용하도록 설계되였다. 어떤것은 정보를 전송하는데서 말단사용자를 돕도록 설계되였으며 또 다른것들은 IP 그자체의 기능을 지원하도록 만들어 졌다. 가장 일반적인 봉사들중의 일부를 아래에 서술한다.

부트규약(bootp)과 동적호스트구성규약(DHCP)

호스트체계에 IP주소를 지정하는데는 3가지 방법이 있다.

수동식 사용자가 특정의 주소를 리용하여 수동적으로 IP호스트를 구성한다.
자동식 봉사기가 설치과정에 자동적으로 특정주소를 호스트에 배당한다.
동 적 봉사기가 설치동안에 동적으로 호스트에 주소들을 배당한다.

수동식방법은 시간이 걸리지만 고장에 안전하다. 그것은 매 IP호스트체계가 IP를 리용하여 통신하는데 필요로 하는 모든 정보들을 가지고 구성될것을 요구한다. 수동식방법

은 같은 IP주소를 유지하여야 하는 체계 또는 IP주소봉사기가 접근할수 있어야 하는 체계에서 리용하기 가장 적당한 방법이다. Web봉사기, 우편봉사기 그리고 IP봉사를 제공하는 다른 봉사기들은 IP통신을 위하여 보통 수동적으로 구성된다.

Bootp는 자동주소배당을 지원한다. Bootp봉사기에 하나의 표가 보관되여 있는데 그것은 매 호스트의 MAC번호를 가지고 있다. 매개 항목은 또한 체계에서 리용될 IP주소들도 포함한다. Bootp봉사기가 IP주소에 대한 요청을 수신할 때 그것은 자기의 표를 참고하여 전송하는 체계의 MAC주소를 찾으며 그 체계에 적당한 IP주소를 돌려보낸다. 이것은 모든 조작의 중심체계에서 수행되므로 관리가 간단하지만 매 MAC주소가 기록되여야 하므로 아직 시간이 걸린다. 또한 리용되지 않는 IP주소공간을 해방시키지 못한다.

DHCP는 자동 및 동적 IP주소배당을 둘 다 지원한다. 주소들이 동적으로 배당될 때 봉사기는 준비되여 있는 번호들의 공간으로부터 IP주소들을 호스트체계들에 넘겨 준다. 자동주소배당에 비한 동적배당의 우점은 하나의 IP주소를 요구하는 호스트에만 하나가 배당된다는것이다. 일단 끝나면 IP주소들은 주소공간에 귀환되여 다른 호스트에 배당될 수 있다.

주　　의

한 호스트가 특정의 IP주소를 유지하는 시간의 크기를 임대주기라고 한다. 짧은 임대주기는 하나의 IP주소를 요구하는 체계만이 하나를 받는다는것을 담보한다. IP가 드문히 리용된다면 작은 주소공간으로 큰 호스트수를 지원할수 있다.

DHCP의 다른 리점은 그 봉사기가 주소정보보다 더 많은것을 보낼수 있다는것이다. 원격호스트는 자기의 호스트이름, 기정경로기, 령역이름, 국부DNS봉사기 등을 가지고 구성될수 있다. 이것은 관리자가 최소작업으로 많은 호스트들에 원격으로 IP봉사들을 구성할수 있게 한다.

하나의 DHCP봉사기는 여러개의 부분망들에 봉사할수 있다.

DHCP의 결함들은 다음과 같다.

- 방송통신량이 증가된것(의뢰기는 주소가 필요할 때 모든 망방송을 전송한다.)
- DHCP봉사기가 정지될 때의 주소공간안정성

많은 체계들에서 누가 망주소에 배당되였는가를 추적하는 표들은 기억기에만 보관되여 있다. 체계가 멎으면 이 표는 없어 진다. 체계를 재시동하면 그전에 다른 체계에 이미 임대하였던 IP주소들이 체계에 배당될수 있다. 이것이 일어 나면 모든 체계에로의 임대를 다시 하거나 임대시간이 끝날 때까지 기다려야 한다.

주　　의

Bootp나 DHCP는 둘 다 통신전송으로서 UDP를 리용한다. 의뢰기는 68의 원천포구로부터 67의 목적지포구에로 주소요청을 전송한다.

령역이름봉사(DNS)

DNS는 호스트이름을 IP주소로 넘기며 또 그 반대로 넘기는 기능을 수행한다. 이것은 Novell의 Web봉사기를 련결할 때 그 체계의 IP주소를 기억할 대신에 WWW.novell.com이라고 입력하면 되게 하는 봉사이다. 모든 IP경로조종은 이름이 아니라 주소로 진행된다. IP체계는 정보를 전송할 때 이름을 리용하지 않지만 사람들은 이름을 기억하기가 더 쉽다. DNS는 원격체계에 보다 더 쉽게 도달하기 위하여 개발되였다. DNS는 사람은 기억하기 쉬운 이름을 입력하고 콤퓨터가 이것을 경로조종 등에 필요한 주소정보로 변환하게 한다.

DNS는 계층적이고 분산적인 구조를 가진다. 인터네트에서 하나의 DNS봉사기가 매 호스트이름의 경로를 유지하는것이 아니다. 매 체계는 일정한 지역에서만 책임을 진다.

그림 3-18은 DNS구조가 어떻게 되여 있는가를 보여 주는 실례이다. 보기에 그것은 하나의 기둥에 아래쪽으로 매달린 수많은 나무와 류사하다. 이 기둥은 인터네트의 골간망을 의미하는것이 아니라 서로 다른 령역들사이의 DNS련결성이 존재한다는것을 지적한다. 기둥 바로 아래에 위치한 체계를 뿌리이름봉사기라고 한다. 매개 뿌리이름봉사기는 하나 또는 몇개의 웃준위령역에 대하여 봉사한다. 웃준위령역의 실례로는 .com, .edu, .org, .mil 또는 .gov 등을 들수 있다. .com으로 끝나는 매개 령역은 같은 웃준위령역의 부분이라고 말한다.

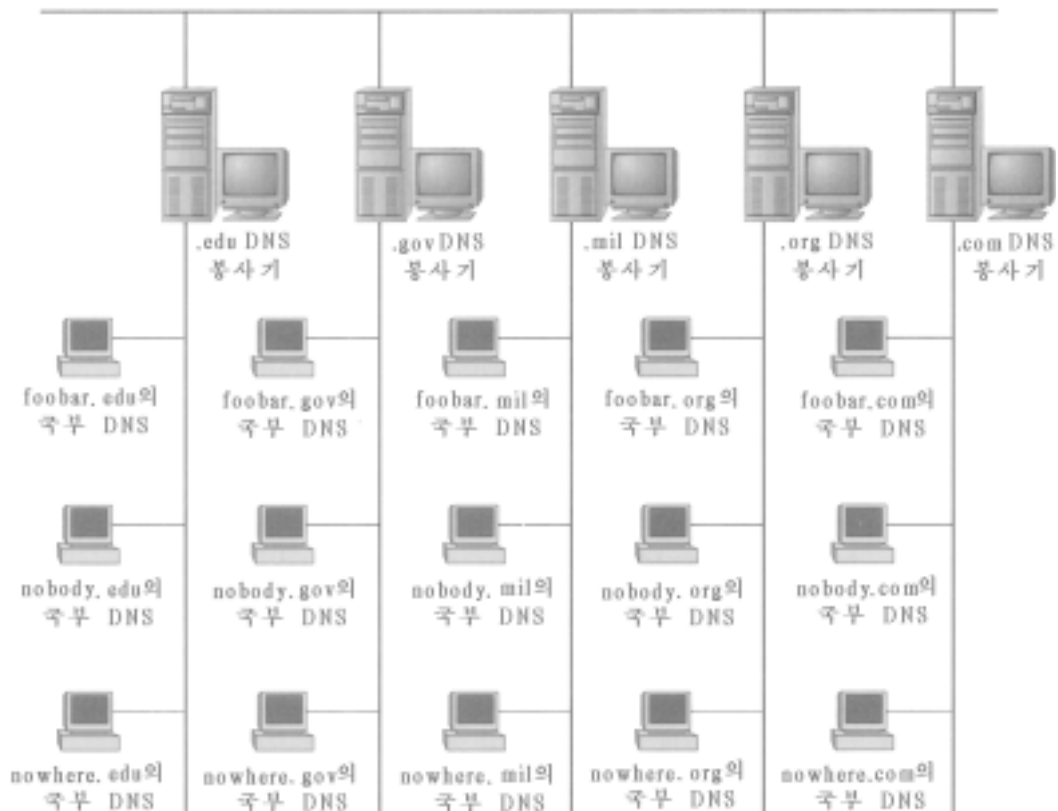



그림 3-18. DNS의 계층적구조

뿌리이름봉사기는 웃준위령역내의 매 부분령역을 위한 DNS봉사기의 경로를 유지할 책임을 맡고 있다. 이것들은 매 부분령역안의 개별적인 체계들에 대하여서는 알지 못하며 다만 그것들을 책임지는 DNS봉사기만을 알고 있다. 매 부분령역 DNS봉사기는 자기령역안의 모든 호스트에 대하여 IP주소를 추적할 책임을 맡고 있다.

그것이 어떻게 동작하는가를 보기로 하자. 만일 foobar.com령역의 성원이라고 하면 Web열람기를 돌려서 다음의 URL을 입력한다.

http://www.sun.com

그러면 체계는 먼저 자기의 DNS캐쉬(그것을 가지고 있다면)를 검사하여 www.sun.com의 IP주소를 찾아 본다. 없다면 그는 하나의 DNS질문(DNS질문은 그저 IP정보를 위한 요청이다.)을 형성하여 foobar.com령역안의 DNS봉사기들중 하나에 그 주소를 요구한다. 그것이 질문한 체계는 ns.foobar.com이라고 가정하자.

만일 ns.foobar.com이 이 정보를 가지고 있지 않다면 그는 또 DNS질문을 구성하여 그 요청을 웃준위령역 .com에 책임이 있는 뿌리이름봉사기에로 보낸다. 그것은 여기에 Sun령역이 위치하고 있기때문이다.

뿌리이름봉사기는 자기의 표들을 참고하고 이와 류사한 하나의 응답을 만든다.:《나는 www.sun.com에 대한 IP주소를 모른다. 그러나 나는 ns.sun.com이 sun.com령역안의 모든 호스트들에 대한 책임을 지고 있다는것을 안다. 그의 IP주소는 10.5.5.1이다. 당신의 질문을 그 체계에로 보내시오.》 이 응답은 다음에 ns.foobar.com에로 보내여 진다.

Ns.foobar.com은 지금 자기가 sun.com령역안의 한 체계를 찾으려면 ns.sun.com에게 물어야 한다는것을 안다. Ns.sun.com은 자기의 표를 참고하여 www.sun.com에 요청을 보낸다.

Ns.sun.com은 자기의 표를 참고하여 www.sun.com에 대한 IP주소를 찾는다. Ns.sun.com은 다음에 ns.foobar.com에게 그 IP주소를 보낸다. 그러면 Ns.foobar.com은 이 정보를 보관하고 그 대답을 당신의 체계에로 전송한다. 체계는 이제 이 IP주소정보를 리용하여 원격Web봉사기에 도달할수 있다.

만일 질문을 많이 하여야 한다고 생각하고 있다면 이 과정에 대한 좋은 리해를 가진것으로 된다. 그러나 보충적인 통신망은 하나의 체계가 인터네트의 모든 체계에 대한 DNS정보를 보관하는데 필요한 추가정보의 량에 비하면 매우 경제적이라고 볼수 있다.

리해한바와 같이 DNS는 질문하는 동안에 캐쉬에 보관한 정보를 효과적으로 리용한다. 이것은 널리 알려 진 싸이트들을 찾을 때 통신량을 감소시키는데 효과적이다. 실례로 foobar.com안의 누군가가 지금 www.sun. com에 도달하려고 시도한다면 이 체계에 대한 IP주소는 ns.foobar.com의 캐쉬에 보관되여 있다. 그러므로 지금 이 질문에 직접 대답할수 있다.

ns.foobar.com이 이 정보를 상기하는 시간의 크기는 이 주소를 위한 수명시간(TTL)에 의하여 결정된다. TTL은 원격이름봉사기를 관리할 책임이 있는 관리자에 의하여 설정된다(이 경우에는 ns.sun.com). 만일 www.sun.com이 안정한 체계라면 이 값은 30일과 같은 높은 값으로 설정될수 있다. 만일 www.sun.com의 IP주소가 자주 변하는것으로 알고 있다면 TTL은 몇시간과 같은 보다 작은 값으로 설정될수 있다.

TTL설정에 대한 경고

TTL설정을 적당히 관리하는것이 왜 중요한가를 알기 위하여 한가지 실례를 고찰하자. foobar.com 등을 위한 우편중계가 체계 mail.foobar. com으로부터 운영된다고 하자. 또한 인터네트로부터 그 망에 들어 오는 DNS질문들의 수를 감소시키기 위하여 30일이라는 큰 TTL값이 설정되였다고 가정하자. 마지막으로 망은 ISP를 변경하여 인터네트와 통신할 때 리용할 새로운 IP번호들의 모임을 배당 받았다고 가정하자.

망이 재주소화될 때 변화가 일어 난다. 즉시 사용자들은 전화호출을 받게 되는데 그들의 주소에로 보낸 우편이 배달오유를 내고 되돌아 오고 있다고 할것이다. 그 오유는 서로 다른데 어떤것은 통과해 가고 어떤 우편은 오유로 없어 진다.

무엇이 잘못되였는가? TTL값이 30으로 설정되였기때문에 원격 DNS 봉사기들은 TTL이 끝날 때까지는 낡은 IP주소를 기억할것이다. 어떤 사람이 변화가 있기전에 foobar.com령역에 우편을 보냈다면 그것은 그들의 DNS봉사기가 다른 하나의 질문을 만들고 그 IP주소가 변화되였다는것을 알기 30일전일수도 있다. 게다가 이 변화에 가장 크게 영향 받는 령역은 우편을 가장 많이 교환하는것들이다.

이 문제를 푸는데는 두가지 방도가 있다.

1. 그것을 무시하고 책상 밑에 감추라. 일단 TTL이 끝나면 우편배달은 정상으로 돌아 올것이다.
2. 우편을 교환하는 매 령역에 대한 DNS관리자와 접촉하여 그들의 DNS캐쉬를 재설정하도록 요구하시오. 이렇게 하면 원격체계는 우편을 보내려고 하는 다음번에 그 주소를 보게 될것이다. 이 선택은 좀 어려운것인데 AOL이나 CompuServe와 같은 큰 령역에서는 불가능하다.

이러한 오유를 피하자면 기초적인 계획화가 필요하다. 변화가 있기 적어도 30일전에 TTL값을 매우 적은 시간(한시간정도)으로 낮추시오. 이렇게 하면 원격체계는 간단한 시간크기에 대한 정보만을 캐쉬에 보관하게 된다. 변화가 끝나면 TTL은 30일까지로 조정되여 통신량을 감소시킬수 있다. 자기들의 호스트이름이나 주소를 변화시키려하지 않는 체계들에 대하여서는 30일이 좋은 TTL값으로 된다.

주 의

DNS는 통신할 때 TCP와 UDP를 리용한다. 둘 다 목적지포구로 53을 쓴다.

하이퍼본문전송규약(HTTP)

HTTP는 Web열람기와 Web봉사기사이의 통신에서 리용된다. 그것은 사용자가 봉사기로부터 정보를 꺼내가는 동안 하나만의 대화를 만들고 유지하지 않는다는데서 대부분의 봉사들과 다르다. 본문이나 도형 또는 음성과 같은 매 정보요청은 개별적인 자기의 대화를 만드는데 일단 그 요청이 끝나면 끝난다.

많은 그림을 가지고 있는 Web페지는 열람기에 싣기 위해서 여러개의 동시적인 련결

을 만들어야 한다. 하나의 Web열람기가 Web봉사기로부터 한 페지를 읽기 위하여 10, 20 또는 지어 50개의 대화를 만드는것도 희귀한 일이 아니다.

판본 1.0에서 HTTP는 자료형식의 교환을 지원하기 위하여 다매체인터네트우편확장(MIME)기능을 포함하였다. 이것은 HTTP가 실제로 교차플래트홈봉사로 되게 하였는데 그것은 MIME가 Web열람기로 하여금 봉사기에게 자기가 어떤 형식의 파일을 지원할수 있는가를 알려 줄수 있게 하기때문이다. MIME는 또한 봉사기가 Web열람기에게 어떤 형식의 자료가 수신되게 되는가를 알려 줄수 있게 한다. 이렇게 하면 열람기는 수신될 자료에 대하여 정확하고 플래트홈에 맞는 보기 또는 실행용쏘프트웨어를 선택할수 있다.

주 의

HTTP는 통신할 때 TCP와 80의 목적지포구를 리용한다.

우편국규약(POP)

우편국규약은 대표적으로 UNIX쉘구좌로부터 우편을 꺼내갈 때 리용된다. 사용자는 그 체계와 telnet련결을 만들지 않고 자기의 우편을 읽을수 있다. 우편을 받기 위하여 자기의 ISP에 전화접속할 때 이것은 UNIX체계로부터 우편을 받기 위하여 POP규약을 리용하고 있는것이다.

UNIX사용자가 전자우편통보문을 받을 때 그것은 보통 /var/spool/mail 등록부에 보관된다. 이 통보문은 보통 그 체계에 원격접속(telnet)하고 mail지령을 돌리면 꺼내갈수 있다. Mail은 쓸모 있는 도구이지만 사용자대면부를 제대로 가지고 있지 못하다. 해보지 못한 사용자에게는 그 명령이 애매한것 같고 기억하기 어렵다.

POP는 사용자가 자기의 사용자이름과 통과암호를 리용하여 체계에 련결하고 자기의 우편을 꺼내갈수 있게 한다. POP는 쉘접근은 허용하지 않는다. 그것은 간단히 사용자가 체계에 남기고 있는 우편통보문을 꺼낼뿐이다.

POP를 지원할수 있는 우편의뢰기는 여러가지가 있으므로 사용자는 가장 좋아 하는 전자우편의뢰기를 선택할수 있다. POP의 최신판은 POP3 이다.

POP3을 리용할 때 사용자는 통보문을 POP봉사기에 남겨 두고 그것들을 원격으로 보든지(직결우편), 또는 그 통보문을 국부체계에 내리적재하고 그것들을 비직결로 읽든지(비직결우편)를 선택할수 있다. 통보문들을 봉사기에 남겨 두면 체계관리자는 그 체계를 복제할 때 모든 사람의 통보문을 중심적으로 복제할수 있다. 그러나 사용자가 자기의 통보문을 지우지 않는다면(12,000개도 넘는 통보문을 가지고 있는 우편함도 있다.) 의뢰기를 위한 적재시간이 너무 길수 있다는것이 결함이다. 매 통보문의 복사가 봉사기에 남아 있으므로 의뢰기가 련결할 때마다 모든 통보문이 내리적재되여야 한다.

비직결방식으로 POP의뢰기를 리용하는것의 우점은 낡은 통보문들을 처리하기 위한 국부폴더를 만들수 있는것이다. 통보문은 국부적으로 보관되므로 많은 통보문들에 대한 적재시간은 비교적 짧다. 이렇게 하면 POP봉사기가 전화련결(dial-up)로 접근된다면 큰 속도개선을 이룩할수 있다. 국부적폴더만이 리용될수 있다는것에 주목하라. POP3은 공유폴더의 리용을 지원하지 않는다.

비직결방식의 결함은 구동기고장으로부터의 회복을 담보하기 위해서 매 국부체계가 복제되여야 한다는것이다. 대부분의 POP의뢰기들은 비직결방식으로 동작한다.

POP3의 가장 큰 결함의 하나는 그것이 전역주소책의 자동생성을 지원하지 않는것이다. 개인주소책만이 리용된다. 실례로 POP3우편체계를 리용하고 있다면 체계의 다른 사용자들의 주소를 자동적으로 보는 방법이 없다.

여기서 두가지 선택을 할수 있다.

- 어떤 다른 수단을 통하여 수동적으로 다른 주소들을 찾아서 개인주소책에 넣을수 있다.
- 체계관리자에게 요구하여 체계의 전자우편주소들의 목록을 만들고 이 목록을 모든 사용자들에게 전자우편으로 보내게 한다.

그러면 매 사용자는 그 파일을 리용하여 자기의 개인주소책을 갱신할수 있다.

특별히 유리한 선택은 없으므로 POP는 주소책이나 폴더를 공유할 필요가 없는 가정 인터네트사용자에게 가장 적합하다. 기업상의 리용을 위해서는 IMAP4규약(다음절에서 고찰)이 가장 적합하다.

POP3의뢰기에 의하여 하나의 통보문이 배달될 때 그 의뢰기는 통보문을 그 POP봉사기에 되돌려 보내거나 중심우편중계기에로 보낸다. 이중에 어느것이 수행되는가 하는것은 POP의뢰기가 어떻게 구성되는가 하는데 달려 있다. 새로운 통보문 또는 응답을 배달할 때 POP의뢰기는 단순우편전송규약 SMTP를 리용한다. POP의뢰기가 아닌 넘겨 주는 체계는 그 통보문의 전송에 결정적인 책임을 진다.

우편발송중계를 리용하여 POP의뢰기는 통보문이 최종목적지에 도달하기전에 망으로부터 떨어 져 나올수 있다. 대부분의 SMTP통보문들은 매우 빨리 배달되지만(1s이하로) 통화중인 우편체계는 한 통보문을 받는데 10min 또는 그이상 걸릴수 있다. 발송체계를 리용하면 원격POP의뢰기가 전화접속을 유지하는데 필요한 시간을 줄일수 있다.

만일 우편중계기가 문제를 만나서(수신자의 전자우편주소를 잘못 입력했다든가 등) 통보문이 전송될수 없게 되였다면 그 POP의뢰기는 다음번에 POP봉사기에 련결할 때 배포오유통지를 받게 된다.

주 의

POP3은 전송층에서 TCP를 리용하고 목적지포구로 110을 쓴다.

인터네트통보문접근규약, 판본 4(IMAP4)

IMAP는 우편국규약의 다음 세대로 설계되였다. 그것은 POP와 같은 특징들을 가지지만 작업집단환경에서 보다 쉽게 확장할수 있는 많은 특징들을 더 가지고 있다.

POP3에서는 사용자가 통보문을 봉사기에 남겨 두고 원격으로 볼것인가(직결우편), 또는 통보문을 내리적재하고 그것을 비직결로 읽을것인가(비직결우편) 하는 선택권을 가지고 있다. 그러나 IMAP는 단절이라고 하는 세번째 선택을 지원한다.

직결방식에서 모든 통보문은 IMAP봉사기에 보관된다. POP우편의뢰기를 직결방식으

로 시동하는것은 통보문이 많을 때에는 시간이 많이 걸리지만 IMAP에서는 기발의 리용에 의하여 이 문제를 극복하고 있다.

알고 있는바와 같이 POP의뢰기가 POP봉사기에 련결할 때 의뢰기는 간단히 인증하고 통보문을 적재하기 시작한다. 봉사기의 모든 통보문들은 새것이고 아직 읽지 않은것으로 간주된다. 이것은 사용자의 전체 내용이 통보문을 읽기전에 전송되여야 한다는것을 의미한다. 그러나 IMAP봉사기에 련결할 때 그것은 현재의 통보문을 인증하고 그것의 기발상태들을 검사한다. 기발들은 통보문이 《보았다》, 《지웠다》, 《대답하였다》 등으로 표식되도록 한다. 이것은 IMAP의뢰기가 전체 우편함을 전송하는것을 피하기 위하여 이미 본 통보문만을 모으도록 구성될수 있다는것을 의미한다.

비직결방식에서 련결시간은 미리보기에 의하여 감소될수 있다. 미리보기는 사용자가 국부체계에로 통보문을 전송하지 않고 모든 새 통보문의 머리부정보를 훑어 볼수 있게 한다. 사용자가 원격으로 특정의 통보문을 가져 가려고 한다면 그는 어느 통보문은 수신하고 어느것은 그대로 남겨 둘것인지를 선택할수 있다. 또한 통보문들을 국부체계에로 전송하지 않고 머리부정보와 파일크기에 따라 그것들을 지워 버릴수도 있다. 이것은 보통 자기우편을 원격으로 꺼내가고 있다면 실제적인 시간절약으로 된다.

IMAP는 POP에서는 지원하지 않는 세번째 련결방식으로 단절이라고 하는 방식을 포함하고 있다.

원격IMAP의뢰기가 단절방식으로 동작하고 있을 때 그는 모든 새로운 통보문들의 하나의 복사만을 꺼내간다. 원본들은 다 IMAP봉사기에 남겨 둔다. 의뢰기가 다음번에 그 체계에 련결할 때 그 봉사기는 캐쉬에 보관된 정보의 어떤 변화에 동기화된다. 이 방식은 몇가지 우점을 가진다.

- 망통신량과 전화접속가입시간이 감소됨으로써 련결시간이 최소화된다.
- 통보문들이 중앙에 위치하고 있으므로 쉽게 여벌복사될수 있다.
- 모든 통보문이 복사기에 기초하고 있으므로 우편은 여러 의뢰기들에 의하여 호출될수 있다.

마지막 우점은 사람들이 항상 같은 콤퓨터를 가지고 일하지 않는 환경에서 매우 쓸모 있다. 실례로 한주에 며칠동안 집에서 일하는 사람들은 자기의 집과 작업콤퓨터사이에서 자기우편의 동기화를 쉽게 유지할수 있다. 대부분의 POP의뢰기와 같이 비직결방식에서 일할 때에는 그의 작업체계가 받은 우편은 그의 가정체계에서는 볼수 없을것이다. IMAP의뢰기는 이러한 제한이 없다.

POP에 비한 또 하나의 개선은 IMAP가 봉사기에 통보문을 쓰는것을 지원한다는것이다. 이것은 사용자가 국부폴더대신에 봉사기에 기초한 폴더를 가질수 있게 한다. 이 폴더들은 단절방식에서도 동기화될수 있다.

IMAP는 또한 집단폴더들을 지원한다. 이것은 우편사용자가 통보문들을 많은 사람들에게 게시할수 있는 게시판구역을 가질수 있게 한다. 이 기능은 NNTP에서의 새 소식과 류사하다(NNTP는 다음에 서술한다.). 집단폴더들은 훌륭한 정보공유수단을 제공한다. 실례로 인사관리부서는 기업방책정보를 위하여 집단폴더를 설정할수 있다. 이렇게

하면 인쇄된 지도서들을 만들 필요가 없어 질것이다.

일러두기

만일 IMAP를 리용하고 있거나 또는 현재의 전자우편체계가 집단폴더들을 지원하고 있다면 Computer support라고 이름을 붙인것 또는 어떤 류사한것을 만드시오. 거기에서 자기의 가장 일반적인 지원호출들에 대한 지원을 제공하는 통보문을 부칠수 있다. 이것은 수신된 지원호출들의 수를 감소시키며 사용자에게 문제를 어떻게 해결할것인가에 대한 서면상의 방향을 줄수 있다. 또한 화면보관도 할수 있는데 이것은 전화로 론의할 때보다 문제를 매우 쉽게 풀수 있게 한다.

IMAP는 응용프로그람구성접근규약(ACAP)과 결합할수 있도록 설계되였다. ACAP는 의뢰기에게 구성정보에로의 접근을 허용하고 중심위치로부터의 우선권을 허용하는 하나의 독립적인 봉사이다. ACAP에 대한 지원은 IMAP의 이식성을 크게 강화한다.

실례로 한주에 며칠은 집에서 일하는 사람들은 자기의 개인주소책과 구성정보도 봉사기에 보관할수 있다. 만일 그가 직장에 있는데 새로운 이름과 전자우편주소를 그의 주소책에 첨부한다면 그 이름은 그가 자기 집의 체계를 리용할 때 준비되여 있을것이다. 이것은 매개 의뢰기가 자기의 개별적인 주소책을 매 국부체계에 가지고 있는 POP에서는 불가능한것이다. ACAP은 또한 임의의 구성변화가 두 체계에 다 영향을 준다는것을 담보한다.

ACAP는 우편관리자에게 우편을 접근할 때 사용자들을 위한 기업표준을 설정하는데서 어떤 조종기능을 제공한다. 실례로 관리자는 누구나 다 접근할수 있는 전역주소책을 설치할수 있다.

주 의

IMAP는 전송층에서 TCP 목적포구143을 리용한다.

망파일체계(NFS)

NFS는 원격파일체계에로의 접근을 제공한다. 사용자는 파일이 국부체계에 위치하고 있을 때 원격파일체계에 접근할수 있다. NFS는 파일접근만을 제공한다. 이것은 처리기시간 또는 인쇄와 같은 다른 기능들은 국부체계가 제공하여야 한다는것을 의미한다.

NFS은 봉사기와 의뢰기 둘 다에 대하여 구성변화를 요구한다. 봉사기에서 공유되여야 할 파일체계는 먼저 수출되여야 한다. 이것은 어느 파일이 공유될것인가를 결정함으로써 수행된다. 이것은 하나의 등록부 또는 전체 디스크일수 있다. 또한 누가 이 파일체계에 접근하였는가 하는것도 정의하여야 한다.

의뢰기쪽에서 체계는 원격파일체계를 설치하도록 구성되여야 한다. UNIX체계에서 이것은 체계의 etc/fstab파일에서 하나의 항목을 만듦으로써 수행되는데 원격체계의 이름, 설치하려는 파일체계 그리고 국부체계의 어디에 그것을 배치하겠는가를 지적하면 된다. UNIX세계에서 이것은 한 등록부아래에 위치한 하나의 등록부구조이다. DOS세계에서는 원격파일체계는 일의적인 구동기문자에 배당될수 있다. DOS와 Windows에서는 NFS를

리용하기 위하여 제3자의 쏘프트웨어가 필요하다.

그것은 편리한 파일공유방법을 제공하지만 많은 기능적결함들을 가지고 있다. FTP와 NetWare의 NCP규약에 비해 볼 때 파일전송시간이 느리다. NFS는 하나의 사용자만이 파일에 쓸수 있도록 담보하는 파일잠금기능을 못 가지고 있다. 너무 한심하지는 않지만 NFS는 정보가 손상없이 수신되였다는 담보를 하지 못한다. 전체의 등록부가 NFS를 리용하여 원격체계에로 복사되다가 수송중에 손상된 경우들도 있다. NFS는 자료의 안전성을 검사하지 않기때문에 파일이 처리될 때까지는 오유를 발견하지 못한다.

주 의

NFS는 UDP를 리용하여 포구 2049를 리용하여 통신한다.

망뉴스전송규약(NNTP)

NNTP는 뉴스를 전송하는데 리용된다. 뉴스는 통보문이 사용자에게가 아니라 뉴스그룹에 전송된다는것을 제외하고는 전자우편과 기능에서 매우 비슷하다. 매 뉴스그룹은 공통적인 특징이나 주제에 따르는 통보문보관구역이다. 우편의뢰기대신에 뉴스의뢰기가 리용되여 각이한 주제구역으로 배달된 통보문들을 읽는다.

실례로 자기의 NetWare봉사기에서 망을 구성하여야 할 문제거리를 가지고 있다고 하자. 이때 뉴스그룹 comp.os.NetWare.connectivity에 배달된 통보문들을 검사하여 누군가가 같은 문제에 대한 풀이를 찾았는가를 알아 볼수 있다. 각이한 주제에 따라 수백수천개의 뉴스그룹이 있을수 있다. 실례로 다음과 같은것들이 있다.

com.protocols
alt.clueless
alt.barney.dinosaur.die.die.die

뉴스우편물들을 읽기 위하여서는 뉴스봉사기에 접근하여야 한다. 뉴스봉사기들은 자기들이 받은 새로운 뉴스들을 다른 봉사기들에 중계함으로써 통보문들을 교환한다. 이 과정은 좀 느린데 새로운 통보문이 매 뉴스봉사기들에 퍼지려면 3~5일의 기간이 걸린다.

뉴스는 매우 자원집약적이다. 하나의 뉴스봉사기는 한주일에 여러 기가비트정도의 정보를 수신한다. 수신, 송신 그리고 낡은 통보문을 제거하는데 요구되는 시간은 많은 CPU시간을 잡아 먹을수 있다.

뉴스는 최근 몇년동안 스팸이라고 부르는 활동에 의하여 그 매력이 감소되였다. 스팸이란 불필요하고 주제도 없는 통보문들을 마구 퍼뜨리는 활동이다. 실례로 이 책을 쓰는 동안에 comp.os.NetWare.connectivity에는 383개의 통보문이 포함되였다. 이중에서 11%는 일확천금계획에 대한 광고이고 8%는 콤퓨터관련장치 또는 봉사에 대한 광고이고 6%는 어떤 문제에 대한 전용자의 의견을 서술한 우편물들이고 다른 23%는 NetWare관련이지만 아무런 련결성도 가지지 않는 광고들이였다. 이것은 우편물의 절반정도가 실제적인 내용을 가지는것이라는것을 의미한다. 어떤 그룹에서는 그 몫이 더 한심하다.

주 의

NNTP는 전송에서 TCP를 리용하며 모든 통신을 위하여 포구 119를 쓴다.

IP 우에서의 NetBIOS

IP에서의 NetBIOS는 원래 봉사는 아니지만 그것은 대화층지원을 첨가하여 NetBIOS 자료흐름을 IP파케트안에 포장할수 있게 한다. 이것은 Windows NT나 Samba를 리용할 때 필요한데 그것은 파일 및 인쇄기공유를 위하여 NetBIOS를 리용한다. 만일 IP가 NT봉사기에 속한 유일한 규약이라면 그것은 포장을 통한 파일공유를 위하여 NetBIOS를 사용하고 있다.

Samba는 UNIX파일체계와 인쇄기들의 공유로써 접근되도록 하는 프로그람묶음이다. 결과적으로 그것은 UNIX체계가 NT봉사기인것으로 보이게 한다. 의뢰기는 다른 UNIX체계이거나(Samba의뢰기를 돌리는) Windows 95/98/NT /2000일수 있다. Windows의뢰기는 NT/2000봉사기와 통신할 때와 같은 구성을 리용하므로 어떤 추가적인 쏘프트웨어를 요구하지 않는다.

Samba의 원천코드는 인터네트에 무료쏘프트웨어(freeware)로 준비되여 있다. UNIX의 15가지 특징보다 더 많은것을 지원하고 있다.

주 의

NetBIOS가 IP안에서 포장될 때 전송층규약으로서 TCP와 UDP가 둘 다 리용된다. 모든 통신은 포구 137-139에서 진행된다.

단순우편전송규약(SMTP)

SMTP는 체계들사이의 우편통보문을 전송하는데 리용된다. SMTP는 통보문교환형련결을 리용한다. 매 우편통보문은 두 체계사이의 대화가 끝날 때까지 그대로 전진한다. 만일 하나이상의 통보문이 전송된다면 매 우편통보문에 대하여 따로따로 대화가 설정되여야 한다.

SMTP는 ASCII본문만을 전송할수 있다. 그것은 복잡한(rich) 본문이나 2진파일 및 그 부속물전송은 지원하지 않는다. 이러한 형태의 전송이 필요할 때에는 그것을 ASCII형식으로 변환하는 외부적프로그람이 필요하다.

이 기능을 제공하는 원래의 프로그람은 uuencode와 uudecode였다. 2진파일은 먼저 uuencode에 의하여 처리되여 ASCII형태로 변환된다. 이 파일은 다음에 우편통보문에 붙어 전송되게 된다. 일단 수신되면 이 파일은 uudecode에 의하여 처리되여 원래의 2진형식을 되찾게 된다.

uuencode/uudecode는 MIME의 리용으로 교체되였다. MIME는 같은 변환과제를 수행하지만 그것은 결과적인 ASCII정보를 압축도 한다. 그 결과는 보다 작은 부속물로서 적은 비용으로 보다 빠른 전송을 할수 있게 한다. Apple콤퓨터들은 Binhex라고 부르는 응용프로그람을 리용하는데 이것은 MIME와 같은 기능을 수행한다. MIME는 지금 대부분의 UNIX와 DC우편체계들에서 지원되고 있다.

Uuencode/uudecode, Binhex, MIME는 서로 호환되지 않는다. 한 원격우편체계와 본

문통보문을 교환하고 있는데 결과가 쓸모없이 끝난다면 아마 서로 다른 변환형식을 리용하고 있을수 있다. 많은 현대적인 우편관문국들은 이러한 통신문제를 해결하기 위하여 uuencode/uudecode와 MIME를 둘다 지원한다. 어떤것은 지어 Binhex도 지원한다.

주 의

SMTP는 통신에서 TCP와 목적포구 25를 리용한다.

단순망관리규약(SNMP)

SNMP는 망장치들을 감시하고 조종하는데 리용된다. 감시 또는 조종국을 SNMP관리국이라고 부른다. 망장치를 조종하기 위하여서는 SNMP대리자를 돌려야 한다. 이 대리자와 관리국이 함께 동작하여 망관리자에게 그 망의 조종의 중심점을 준다.

주 의

SNMP대리자는 망장치에로의 련결을 제공한다. 그 장치는 관리가능한 집선기, 경로기 또는 봉사기일수도 있다. 대리자는 관리국에 보고할 때 정적 및 동적정보를 다 리용한다.

정적정보는 장치를 유일하게 식별하기 위하여 그안에 보관되여 있는 자료이다. 실례로 관리자는 SNMP정적정보의 부분으로서 장치의 물리적위치와 계렬번호를 보관할수 있다. 이것은 SNMP관리국으로부터 어느 장치와 작업하고 있는가를 쉽게 식별할수 있게 한다.

동적정보는 그 장치의 현재의 상태와 관련한 자료이다. 실례로 집선기의 포구는 그것이 제대로 동작하는가에 따라 가능 또는 금지될수 있으므로 그것의 상태를 동적정보로 볼수 있다.

SNMP관리국은 SNMP대리자를 돌리는 모든 망장치들을 조종하는데 리용되는 중앙조종탁이다. 관리국은 우선 관리정보기지(MIB)를 리용하여 망장치에 대하여 배운다. MIB는 망장치제작자에 의하여 제공되는 쏘프트웨어인데 보통 플로피디스크로 제공된다. MIB가 관리국에 첨가되면 그것은 망장치들에 대하여 관리국에 알려 준다. 이것은 한 제작자가 만든 SNMP관리국이 다른 제작자가 만든 망장치들에서 제대로 돌아 가게 담보하는데서 도움이 된다.

정보는 SNMP관리국에 의하여 보통 폴링(polling)을 통하여 수집된다. SNMP관리국은 매 망장치들의 상태를 검사하기 위하여 미리 설정된 구간들에서 질문들을 보낸다. SNMP은 정보를 수집하기 위하여 두개의 명령 get와 getnext만을 지원한다. get명령은 관리국이 특정한 동작파라메터에 대한 정보를 검색할수 있게 한다. 실례로 관리국은 한 경로기에 그것의 포구들중 하나의 현재상태를 보고할것을 요구할수 있다. getnext명령은 장치로부터 완전한 상태를 수집할 때 리용된다. get명령들이 한렬을 보낼 대신에 getnext는 한 장치가 보고할수 있는 매 정보토막들을 련속적으로 검색하는데 리용된다.

SNMP은 또한 명령 set를 통하여 망장치의 조종을 한다. set명령은 망장치의 동작파

라메터 등을 변경하는데 리용된다. 실례로 get명령이 경로기의 포구 2가 금지되였다고 보고한다면 그 경로기에 set명령을 보내여 그 포구를 가능으로 바꿀수 있다.

SNMP는 보통 망장치의 관리도구와 같은 대역의 조종을 제공하지 않는다. 실례로 경로기의 포구들을 열거나 막거나는 할수 있어도 IP망구조를 초기화하거나 포구에 IP주소를 할당하는것은 할수 없다. SNMP에 준비되여 있는 조종의 크기는 제작자의 MIB에 어떤 명령들이 포함되여 있는가 하는것과 SNMP 그자체의 명령구조에 의하여 제한된다. SNMP의 중요한 의미단어는 《간단하다》는것이다. SNMP는 망장치들에 대하여 최소량의 조종만을 제공한다.

대부분의 보고는 SNMP관리국이 망장치들을 폴링하는것으로써 수행되지만 SNMP는 망장치가 중요한 사건들에 대해서는 즉시 관리국에 보고하도록 한다. 이 통보문들을 트랩(trap)이라고 부른다. 트랩들은 그 장치가 다시 폴링될 때까지 기다릴수 없는 중요한 사건이 발생하였을 때 전송된다. 실례로 전원이 방금 차단되였다면 경로기는 SNMP관리조종탁에 하나의 트랩을 보낼수 있다. 이 사건은 망련결성에 중대한 충격을 줄것이므로 그 장치가 다시 폴링될 때까지 기다리지 않고 즉시 SNMP관리국에 보고한다.

주 의

SNMP는 통신할 때 UDP와 목적지포구 161, 162를 리용한다.

Telnet

Telnet는 망의 어떤 다른 체계와의 원격통신대화가 요구될 때 리용된다. 그것의 기능은 대형콤퓨터말단기 또는 원격조종대화와 류사하다. 국부체계는 화면갱신만을 제공하는 피동말단기처럼 된다. 원격체계는 파일체계와 프로그람들을 돌릴 때 필요한 모든 처리시간을 제공한다.

주 의

Telnet는 TCP를 리용하며 목적지포구 23을 쓴다.

WHOIS

WHOIS는 특정의 령역에 대한 정보를 모으는데 리용되는 하나의 도구프로그람이다. 이 도구프로그람은 보통 체계 rs.internic.net에 련결하여 한 령역에 대한 관리적접촉정보와 뿌리봉사기들을 보여 준다.

이것은 특정의 령역이름을 어느 기관이 사용하고 있는가를 알려고 할 때 쓸모 있다. 실례로 명령

whois.sun.com

이라고 입력하면 그 령역과 관련되는 다음의 정보를 얻는다.

Sun Microsystems Inc.（Sun）Sun.com，192.9.9.1
Sun Microsystems Inc.（Sun−DOM）Sun.com

다음의 명령

whois sun−dom

을 또 입력하여 더 탐색하면 추가적인 정보가 더 얻어 진다.

Sun Microsystems，Inc．（SUN−DOM）
2550 Garcia Avenue
Mountain View，CA 94043
Domain Name ：SUN．COM
Administrative Contact，Technical Contact，Zone Contact ：
Lowe，Fredrick（0FL59）Fred．Lowe@SUN．COM
408−276−4199
Record last updated on 21−Nov−96
Record created on 19−0Mar−86
Database last updated on 16−Jun−97 05 ：26 ：09 EDT
Domain servers in listed order ；
NS．SUN.COM 192，9．3
VGR ARL.MIL 128.63.2.6，128.63，16.6，128，4.4
The InterNIC Registration Services Host contains ONLY Internet
Information
（Networks，ASN’s，Domains，and POC’s）
Please use the whois server at nic．ddn mil for MILNET Information

WHOIS는 매우 강력한 고장수리도구로 쓸수 있다. 지금 누가 그 령역을 관리하는데 책임이 있으며 어떻게 그들과 접촉하며 어느 체계가 기본이름봉사기로 간주되는가 하는 것들을 알고 있다. 그러면 nslookup과 같은 DNS도구들을 리용하여 Sun의 우편체계 지어 그들의 Web봉사기의 IP주소도 알아 낼수 있다.

주 의

WHOIS는 통신대화를 만들 때 TCP와 목적지포구 43을 리용한다.

IRC

IRC규약(Internet Relay Chat)는 의뢰기들이 실시간으로 통신할수 있게 한다. 그것은 IRC봉사기들로 된 여러가지 개별적인 망들로 이루어 져 있다. 사용자는 하나의 망에 있는 봉사기에 그들을 련결하는 하나의 의뢰기프로그람을 돌린다. 봉사기는 정보를 같은 망에 있는 봉사기들사이에서 중계한다. 일단 IRC봉사기에 련결되면 사용자에게 하나 또는 몇개의 화제통로가 주어 진다. 통로이름들은 보통 #irchelp와 같이 하나의 #를 가지는데 주어 진 망의 모든 봉사기가 같은 통로표를 공유하므로 그 망우의 어떤 봉사기에 련결한 사용자는 다른 사용자와 통신할수 있게 된다.

주 의

기호 #대신에 &으로 시작하는 통로들은 주어 진 봉사기만에 해당되는것이며 그 망의 다른 봉사기들과 공유되지 않는다.

매개 RIC의뢰기는 유일한 별명(nick)에 의하여 다른 의뢰기들과 구별된다. 봉사기들은 매 의뢰기들에 대하여 그 의뢰기가 돌아 가는 호스트의 실제이름, 그 호스트의 의뢰기의 사용자이름 그리고 그 의뢰기가 련결된 봉사기 등을 포함하여 보충적인 정보를 저장한다.

조작자란 IRC망의 관리를 수행할 능력을 부여 받은 의뢰기들을 말하는데 실례로 어떤 망 경로조종문제를 수정하는데 필요한 련결차단 및 재련결 등을 수행한다. 조작자는 또한 련결을 차단함으로써 망으로부터 어떤 의뢰기를 강제적으로 제거할수도 있다. 조작자는 봉사기에 지정되거나 또는 통로에 지정될수 있는데 그들은 별명이름뒤에 @기호를 붙여서 식별한다.

주 의

IRC는 TCP와 UDP를 둘다 리용할수 있으며 가장 현대적인 IRC봉사기들은 포구 6667-7000에서 대기한다.

웃층의 통신

대화층의 우에 있는 층들을 고찰하면 우리의 통신은 우리가 리용하고 있는 프로그람에 아주 가까운것으로 된다는것을 알수 있다. 표현층과 응용층의 책임은 아래에서 리용되고 있는 규약보다는 보다 더 봉사의 형식을 가지는 기능들이다. 자료변환이나 암호화는 이식가능한 특징으로 간주된다.

주 의

이식가능하다는것은 이 특징들을 아래의 규약을 고려함이 없이 쉽게 다른 봉사들에 적용할수 있다는것을 의미한다. 자료를 전송하는데 IP를 리용하는가 IPX를 리용하는가 하는것은 문제가 되지 않으며 이 특징들을 실현하는 능력은 리용되고 있는 응용프로그람에 의존한다.

실례로 Lotus는 우편통보문들을 전송하기전에 암호화할 능력을 가지고 있다. 이 능력은 그 프로그람의 표현층에서 실현된다. 우편체계를 TCP, SPX 또는 모뎀을 통하여 련결하는가 하는것은 문제로 되지 않는다. 암호화기능은 세개의 규약모두에 의하여 준비되여 있는것이나 갈다. 왜냐하면 그 기능은 그 프로그람자체에 의하여 준비되여 있기때문에 Lotus는 밑에 놓인 규약에 의존하지 않는다.

요 약

이 장에서는 이써네트프레임을 해부하고 국부적이써네트토막에 있는 체계가 어떻게 통신하는가를 고찰하는것으로 시작하였다. 또한 큰 망환경에서 경로조종이 통신을 돕는데 리용되는가를 보았다. 여기서 우리는 여러가지 련결설정방법들을 보았으며 IP봉사들을 고찰하는것으로 이 장을 끌내였다. 이 기술들을 좀 더 깊이 고찰하려면 다음의 책을 참고하길 바란다.

Multiprotocol Network Design and Troubleshooting(Sybex, 1997)

다음 장에서는 일상적인 통신에서 제기되는 몇가지 불안정점들을 살펴 보는것으로 시작한다. 핵심망설계안에 보안을 설치하는것이 어떻게 성능을 개선할뿐아니라 망자료가 공격의 영향을 적게 받게 할수 있는가를 고찰할것이다.

제4장. 위상구조적인 보안

이 장에서는 망전송의 통신특성들을 보기로 한다. 또한 일상적인 망통신에서 어떤 불안전성이 있는가 그리고 이러한 문제들을 완화시키는 망기반구조를 어떻게 개발할수 있는가를 보기로 한다.

망전송에 대한 리해

암호화표준을 설정할 의무를 지니고 있는 국가기관이 국가와 관계되는 암호화된 전송문들을 감시하고 암호를 푸는 책임도 지니고 있다는것은 우연한 일이 아니다. 어떻게 하면 보다 안전하겠는가를 알기 위하여서는 어떤 취약점들이 존재하며 이것들이 어떻게 리용될수 있는가를 리해하여야 한다. 이와 같은 생각을 망통신에 적용한다. 망기반구조에 보안을 설계해 넣을수 있도록 하기 위하여서는 어떻게 망에 련결된 체계들이 서로 통신하는가를 알아야 한다. 많은 공격자들은 기초적인 통신특성들을 리용한다. 만일 이 통신특성들을 알고 있다면 그것들이 나쁘게 리용되지 않도록 담보하기 위한 조치를 취할수 있다.

수자식통신

수자식통신은 모르스부호 또는 이전의 전신체계와 류사하다. 전송과정에 일정한 임풀스패턴들이 리용되여 여러가지 문자들을 표현한다.

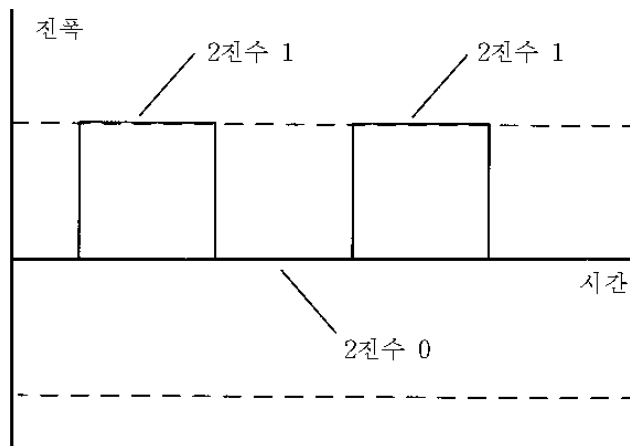



그림 4-1. 시간축에 따라 그린 수자식전송

그림 4-1을 보면 수자식전송의 한가지 실례를 알수 있을것이다. 전압이 전송매체에 가해 질 때 이것은 2진수 1로 간주된다. 신호가 없으면 2진수 0으로 해석된다.

이 파형은 예측가능하고 허용가능한 값들사이의 변화가 크므로 전송의 상태를 결정하는 것은 쉽다. 이것은 신호가 전기신호인 경우에 중요하다. 그것은 회로에 잡음이 가해 지면 전압값을 약간 구부러 지게 할수 있기때문이다. 그림 4-2에서 보는바와 같이 회로에 잡음이 있을 때에도 신호의 어떤 부분은 아직 2진수 1이고 어떤 부분은 0이라는것을 알수 있다.

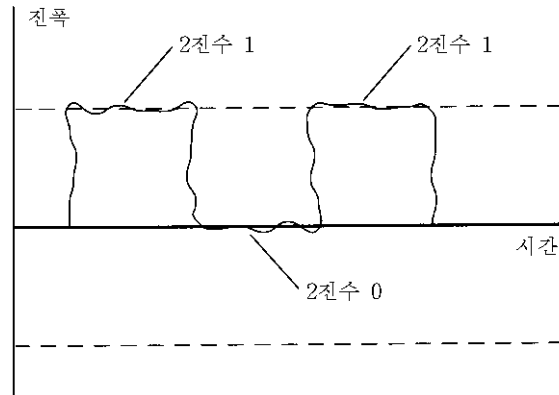



그림 4-2. 잡음 있는 회로에서의 수자식통신

수자통신이 잡음에 강하게 되도록 하는 이 간단한 형식은 또한 그것의 가장 큰 결함으로도 될수 있다. ASCII문자 A에 대한 정보는 하나의 상사형파 또는 진동에 의하여 전송될수 있지만 2진식 또는 수자식등가물을 전송하는것은 8개의 개별적인 파형들 또는 진동들을 요구한다(01000001을 전송하기 위하여). 이러한 고유한 부족점에도 불구하고 수자식통신은 보통 상사식회로보다 훨씬 더 효과적이다. 상사식에서는 잡음 있는 전송을 검출하고 수정하는데 많은 부가처리가 소비된다.

주 의

부가처리(overhead)는 수신하는 체계가 정확한 자료를 받는다는것 그리고 자료가 오유 없다는것을 담보하기 위하여 전송되여야 하는 추가적인 정보의 크기이다. 보통 부차적정보가 많으면 실제 자료를 전송하는데는 보다 적은 대역너비가 차례진다. 이것은 짐을 나를 때 리용되는 포장과 비슷하다. 실례로 수백개의 작은 발포수지알들을 요구하지 않았지만 그것들은 물건이 안전하게 운반되는것을 담보하기 위하여 통안의 공간을 차지하고 있는것이다.

하나의 전기회로(꼬임쌍선을 리용하는 이써네트망과 같은)를 가지고 있을 때 정보를 전송하기 위하여서는 전압을 진동시켜야 한다. 이것은 전압상태가 부단히 변하고 있다는것을 의미하며 이것은 바로 첫 불안전점 즉 전자기간섭을 일으킨다.

전자기간섭(EMI)

EMI는 상사 또는 수자식통신과 같은 교류신호를 사용하는 회로들에서 생긴다. EMI는 일정한 전압준위를 유지하는 회로들에서는 생기지 않는다.

실례로 만일 자동차축전지로부터 나오는 하나의 선을 갈라 내고 그 선으로 움직이는

전자들을 볼수 있다면 항상 움직이고 균일하게 흐르는 안정한 흐름을 보게 될것이다.

그 전압준위는 결코 변하지 않고 언제나 12V이다.

차축전지는 전압준위가 안정하므로 직류회로의 한가지 실례로 된다.

이제 집안의 전등에로 가는 선을 갈라 내고 같은 실험을 한다고 하자. 선에서의 전압값은 측정하는 시간에 따라 그 값은 −220V와 +220V사이에 있다는것을 알것이다. 이 회로의 전압준위는 부단히 변하고 있다. 시간에 따라 그리면 전압준위는 상사신호와 류사할것이다.

교류도선에서 전자들의 흐름을 본다고 할 때 매우 흥미 있는 현상을 알게 될것이다. 전압이 변하고 전류가 흐를 때 전자들은 주로 도선의 겉면으로 흐르려고 한다. 도선의 중심점은 전자운동이 거의 없다는것을 보여 줄것이다. 전원의 주파수를 증가시킨다면 더 욱더 많은 전자들이 중심쪽에서가 아니라 도선의 겉면우에서 흐를것이다. 이 효과는 물스키에서 일어 나는 현상과 얼마간 류사하다. 배가 더 빨리 갈수록 물스키선수는 물면우로 더 높이 뜨게 된다.

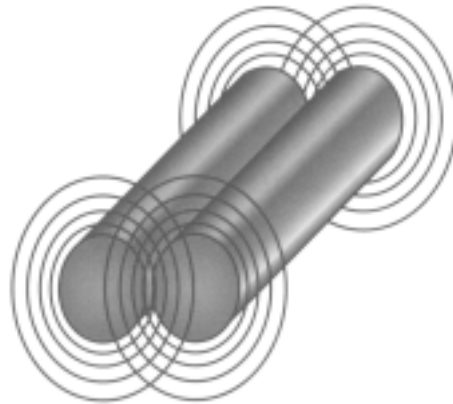



그림 4−3. EMI를 일으키는 교류전류를 나르는 도체

전력주파수가 증가하면 전류흐름에 90° 각을 지어 에네르기가 방출되기 시작한다. 바위가 물면에 부딪칠 때 물결이 이는것과 같은 방식으로 에네르기는 도선의 중심으로부터 밖으로 움직인다. 이 에네르기방출은 도선우의 신호와 직접적인 관계를 가진다. 만일 전압준위 또는 주파수가 증가한다면 방출된 에네르기량도 증가한다(그림 4−3을 보시오).

이 에네르기는 자기적성질을 가지며 그것은 전자석과 변압기가 어떻게 동작하는가 하는 기초로 된다. 도선으로 흐르는 신호를 《냄새 맡기》 위하여 전자기적복사를 측정할수 있다. 전기기술자들은 이러한 목적에 쓰는 도구를 오래전부터 가지고 있었다. 전기기술자들은 간단히 도선주위로 련결할수 있는 장치를 가지고 가운데 있는 도체에로 흐르는 신호를 측정하고 있다.

전기적망케블로부터 나오는 EMI복사를 측정할수 있는 보다 정교한 장치들이 많으며 실지로 그 도선을 흐르는 수자식임풀스들을 기록할수 있다. 이 임풀스들을 일단 기록하면 그것들을 2진형식으로부터 사람이 읽을수 있는 형식으로 변환하는것은 간단한 문제이다.

주 의

꼬임쌍선은 값이 눅은것으로 하여 널리 쓰이게 되였는데 그것도 매우 불안전하다. 대부분의 현대망들은 비차페형꼬임쌍선을 리용하여 배선된다. 꼬임쌍선은 전기신호를 전송하는것이므로 EMI가 발생된다. 케블은 차페를 하지 않았기때문에 매 도체로부터 복사되는 EMI를 매우 쉽게 검출할수 있다. 꼬임쌍선은 일반적인 망을 위하여서는 훌륭한 선택이지만 그 선으로 전송되는 정보가 100% 안전하여야 한다면 그것은 그리 좋은 선택이 못된다.

그러므로 첫번째 취약점은 실제적으로 쓰이고 있는 망케블이다. 사람들이 망의 보안을 평가할 때 이것들은 흔히 빼놓는다. 흔히 콤퓨터실의 천정으로는 거미줄같은 케블들이 지나갈수 있다. 망이 같이 쓰는 사무실공간에 위치하고 있고 공동구역을 통하여 지나가는 케블들을 가지고 있다면 이것은 또 하나의 문제거리로 된다.

이것은 공격자가 민감한 정보들을 수집하기 위하여 콤퓨터실이나 배선실가까이에 가지 말아야 한다는것을 의미한다. 접이식사다리나 떨어 진 천정타일 등은 다 망에 접근점을 만드는데 필요한것들이다. 령리한 공격자는 수집한 정보를 무선송신기를 리용하여 다른곳에 중계할수 있다. 이것은 공격자가 다른 시간에 안전하게 정보수집을 계속할수 있다는것을 의미한다.

빛섬유케블

빛섬유케블은 직경이 62.5μm인 원통형유리실속심을 겉씌우개로 감싼 형태로 되여있다. 겉씌우개는 속심을 보호하며 빛을 유리전도체로 다시 반사하는 역할을 한다. 이것을 다시 질긴 케블과 섬유로 된 씌우개로 감싼것이다.

그리고 이 전체를 다시 폴리염화비닐로 싸거나 또는 그대로 쓴다. 이 바깥씌우개의 직경은 125μm이다. 이러한 직경값으로 하여 이 케블을 때로 62.5/125케블이라고 부른다. 유리로 된 속심은 깨질수 있으므로 케블과 섬유로 된 씌우개를 씌움으로써 빛섬유케블을 원만히 다룰수 있게 하였다. 그림 4-4는 빛섬유케블을 보여 준다.

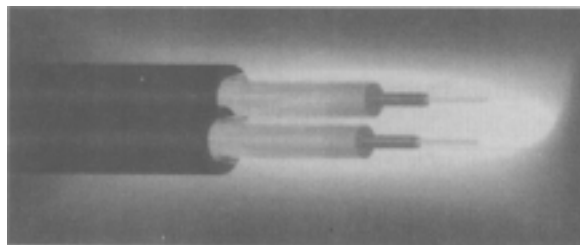



그림 4-4. 빛섬유케블을 벗겨 본것

꼬임쌍선과 달리 빛섬유케블은 자료전송을 위하여 광원을 리용한다. 이 광원은 주로 가시적외선대역에서 신호를 내는 발광2극소자(LED)이다. 케블의 다른쪽 끝에는 LED신호를 수신하는 또 하나의 2극소자가 있다. 빛전송방식에는 두가지 형식 즉 한파모습과

다중방식이 있다.

경 고

동작중의 빛섬유케블묶음을 절대 들여다 보지 마시오. 빛의 세기가 매우 높으므로 눈이 멀수 있다. 만일 케블을 눈으로 봐야 한다면 먼저 그것이 망에서 완전히 차단되였는가를 확인하여야 한다. 케블이 한 순간동안 어둡다고 하여 이것이 동작중이 아니라는것을 의미하지는 않는다. 케블이 완전히 차단되였는가를 알지 못하면 한 눈이 멀수 있는 위험은 매우 크다.

빛분산

가까운 벽에 대고 손전등을 비친다면 빛이 분산한다는것을 보게 된다. 즉 벽에 비친 빛패턴은 손전등의 렌즈보다 큰 직경을 가진다. 만일 두개의 손전등을 함께 그 벽에 비친다면 어느 광원이 비치는것인지 결정하기 어려운 중간위치에 애매한 구역이 있다는것을 알수 있을것이다. 벽으로부터 멀어 지는 방향으로 움직인다면 이 애매한 구역은 더 커진다. 이것은 사실상 다중방식에서 거리가 제한된다는것을 의미한다. 케블의 길이가 증가할수록 수신하는쪽의 2극소자가 서로 다른 빛주파수들을 구별하는것은 더 어려워 진다.

한파모습빛섬유는 하나의 빛주파수를 내보내는 하나의 LED로 이루어 져 있다. 이 단일주파수는 케블의 한 끝으로부터 다른 끝으로 자료를 전송하기 위하여 수자식형태의 임풀스로 된다. 다중방식에 비한 한파모습빛섬유의 리점은 보다 빠르고 보다 긴 거리를 갈수 있다는것이다(수십마일정도). 결함은 장치가 매우 비싸고 설치가 오랜것이다. 회사이름이 단어《Telephone》이나 《Utility》로 끝나는것이 아니라면 한파모습빛섬유는 너무 과분한것이라고 볼수 있다.

다중방식전송은 여러개의 빛주파수들로 구성되여 있다. 빛대역이 한파모습처럼 정확할것을 요구하지 않으므로 다중방식의 장치가격은 한파모습보다 매우 눅다. 다중방식의 결함은 빛분산 즉 빛이 전파될 때 빛선묶음들이 퍼져 나가는 경향이 있는것이다.

다중방식전송은 전기적인것이 아니라 빛에 기초한것이므로 빛섬유는 EMI의 모든 형태로부터 완전히 영향을 받지 않는다는 우점을 가진다. 여기서는 신호가 전도체를 통과할 때 복사가 없다. 유리전도체를 다치기 위하여 씌우개부분을 자를수는 있으나 이것은 체계를 고장내므로 공격자를 실망케 할것이다. 그러나 새로운 빛섬유체계들은 보다 탄력있고 이러한 종류의 공격에는 잘 견디여 내게 되여 있다.

빛섬유케블은 또 한가지 우점을 가지고 있다. 그것은 큰 대역너비의 련결을 지원할수 있다. 10MB, 100MB 그리고 기가비트이써네트는 모두 빛섬유케블로 지원할수 있다. 보안문제와 관련하여서도 성능개선이 있다. 이것은 망에서 빛섬유케블을 리용하는 정당성을 쉽게 증명하게 될것이다. 그것은 대역너비와 보안문제에서 다 만족스러운 결과를 준다. 용감한 공격자가 망에 접근하여 전송을 감시하려고 한다면 그는 많은 통신량을 가진 한 망토막

을 골라내여 큰 자료량을 수집하려고 할것이다. 그런데 마침 이것들은 망에서 이 점을 통하여 흐르는 큰 자료량을 지원하기 위하여 빛케블을 쓰려고 했던 그 토막들이다. 이 토막들에서 빛케블을 씀으로써 자기의 케블기반구조의 완전무결성을 보호할수 있게 된다.

속박 및 비속박전송

공간은 비속박매체라고도 부르는데 형태적인 경계를 가지지 않는 하나의 회로이다. 여기서는 신호가 어떤 경로를 따라 흘러야 한다는 제한이 없다. 꼬임쌍선이나 빛섬유케블은 속박매체의 실례들로서 이것들은 신호가 도선안으로 흐르도록 제한하고 있다. 비속박전송에서는 어디로나 자료를 전송할수 있다.

비속박전송에서는 많은 보안문제가 제기된다. 신호는 그것을 어떤 일정한 지역안에 한정시킨다는 제한을 가지지 않으므로 감시나 도청을 당하기가 더 쉽다. 공간은 여러가지 신호형태들을 전송할수 있다. 가장 널리 리용되는것은 빛과 무선파이다.

빛전송

공간을 통한 빛전송은 망신호를 전송하고 수신하는데 레이자를 리용한다. 이 장치들은 유리매체가 없다는것을 내놓고는 빛케블회로와 류사하게 동작한다.

레이자전송은 집초된 빛묶음을 리용하므로 이것들은 깨끗한 시각선과 장치들사이의 정확한 배당을 요구한다. 이것은 신호가 감시될수 있는 물리적구역을 엄격히 제한하므로 체계의 보안을 강화하는데 도움이 된다. 그러나 공간은 빛전송의 유효거리를 제한하며 결국 그것이 리용될수 있는 경우들의 수도 제한한다.

비속박빛전송은 환경조건에 민감하다. 짙은 안개나 눈이 내리는것은 전송특성에 영향을 줄수 있다. 이것은 빛에 기초한 회로를 차단함으로써 사용자봉사를 거부하는것이 매우 쉽다는것을 의미한다. 그렇지만 공간을 통한 빛전송은 물리적케블을 리용할수 없을 때 비교적 안전한 전송매체로 간주되고 있다.

무선파

망목적으로 리용된 무선파는 주로 1-20GHz대역에서 전송되며 초고주파신호라고 부른다. 이 신호들은 특성상 고정된 주파수 또는 분산스펙트르일수 있다.

고정된 주파수신호 고정된 주파수신호는 전송하려는 정보를 위한 반송파로 리용되는 하나의 주파수신호이다. 라지오방송국은 단일주파수전송의 좋은 실례이다. 라지오방송국의 반송파주파수에 FM다이얄을 동조시키면 그우에 타고 있는 신호를 들을수 있다.

반송파란 다른 정보를 나르는데 리용되는 신호이다. 정보는 그 신호우에 덧놓이게 되며(잡음도 같은 방법으로 덧놓인다.) 결과적인 파가 공간으로 전송된다. 이 신호는 다음에 복조기라고 부르는 장치에서 수신되는데(사실상 자동차용라지오는 여러 주파수들에 설정될수 있는 복조기이다.) 이것은 반송파신호를 제거하고 나머지정보만을 통과시킨다. 반송파신호는 신호의 출력을 증대시키며 그 신호의 수신대역을 확장하기 위하여 리용된다.

고정된 주파수신호는 감시하기 매우 쉽다. 공격자가 반송파주파수를 알고 있다면 그는 전송한 신호를 수신하는데 필요한 모든 정보를 아는것으로 된다. 또한 신호를 방해함

으로써 모든 전송을 차단할수 있는 정보도 가지고 있는것으로 된다.

분산스펙트르신호 분산스펙트르신호는 여러개의 주파수들이 전송된다는것을 내놓고는 고정주파수신호와 같다. 여러 주파수들이 전송되는 리유는 잡음에 의한 간섭을 줄이기 위한데 있다. 분산스펙트르기술은 전쟁기간에 개발되였는데 고정된 주파수로 전송되는 신호를 적들이 같은 주파수를 가지는 신호로 전송하여 방해한것으로부터 생겨 났다. 분산스펙트르는 여러 주파수들을 리용하므로 혼란시키기가 보다 어렵다.

《보다 어렵다.》라는 말에 주의를 돌려야 한다. 분산스펙트르신호를 감시하거나 방해하는것은 아직 가능하다. 신호는 어떤 주파수대역에서 변화하는데 이 대역은 보통 반복되는 패턴을 가진다. 공격자가 주파수변화의 패턴과 시간관계를 알면 그는 전송을 감시하거나 방해할수 있는 위치에 있는것으로 된다.

주 의

무선신호를 감시 또는 방해하는것이 쉽기때문에 대부분의 전송은 도청방지를 위한 암호화에 의거하여 바깥측에 의하여 감시될수 없게 한다. 암호화는 제9장에서 취급한다.

지상전송 대 공간전송 고정주파수 및 분산스펙트르신호를 전송하는데 두가지 방법이 있다. 이것들은 지상전송과 공간전송이라고 부른다.

지상전송: 지상전송은 완전히 륙지에 기초하여 무선신호를 취급한다. 송신국은 주로 산꼭대기나 높은 건물에 위치한 전송탑이다. 이 체계의 대역은 보통 시야선범위이며 막히지 않은 공간을 필요로 하지 않는다. 신호세기에 따라 다르지만 지상전송체계에서는 50mile이 보통 도달가능한 최대범위이다. 지역 텔레비죤 및 라지오방송국이 지상전송에 기초한 방송의 좋은 실례로 된다. 이 신호들은 해당 지역들에서만 수신될수 있다.

공간전송: 공간전송은 지상전송에 그 기초를 두고 있지만 그것은 웃공간에서 지구를 돌고 있는 하나 또는 몇개의 위성을 리용하는것이다. 공간전송의 가장 큰 리점은 대역이다. 신호들은 세계의 거의 모든 구석들에서도 수신될수 있다. 공간전송위성들은 유효방송지역을 크게 하거나 작게 하도록 조절될수 있다.

물론 신호의 방송지역이 클수록 더 잘 감시당할수 있다. 신호대역이 커질수록 신호를 감시하기에 충분한 지식을 가진 사람이 그 방송구역안에 있을 가능성은 더 커질것이다.

전송매체선택

망으로 자료를 전송하는 매체를 선택할 때 많은 보안관련문제들을 고려하여야 한다.

자료가 얼마만한 가치가 있는가

앞의 장들에서 본바와 같이 전형적인 공격자는 망을 공격함으로써 무엇인가를 얻으려 한다. 만일 금융정보를 포함하는 자료기지를 가지고 있다면 그것은 물리적공격을 기도할만큼 충분한 가치가 있는것으로 된다.

어느 망로막이 민감한 자료를 나르는가

망은 일상적으로 민감한 자료를 나르고 있다. 이 정보를 보호하기 위하여서는 그것이 어떻게 리용되는가 하는 작업흐름을 알아야 한다. 실례로 만일 회사의 회계자료를 민감한것이라고 본다면 어떻게 그 정보가 보관되며 누가 그것에 접근하는가를 알아야 한다. 자기의 국부적봉사기를 가지고 있는 작은 작업집단은 비속박매체를 리용하여 원격설비로부터 접근되는 구좌자료기지보다는 훨씬 안전할것이다.

일러두기

> 자기의 시설들사이로 지나가는 봉사형태들을 분석하는데 주의를 돌려야 한다. 실례로 전자우편은 보통 크게 주의를 돌리지 않는데 그것은 다른 사무봉사들보다 기업에 대한 더 많은 정보를 포함할수도 있다. 대부분의 전자우편체계는 통보문을 평문으로 전송하므로(만일 공격자가 이 자료흐름을 포착한다면 그 내용을 인차 알수 있다.) 전자우편은 망봉사에서 가장 잘 지켜야 하는 대상의 하나로 되여야 한다.

침입자가 발견될것인가

집단이 3~4명으로 구성되여 있다면 침입자를 찾기 쉽다. 이것을 3천 또는 4천으로 확대하면 문제는 그것에 비례하여 어려워 진다. 만일 망관리자라면 자기 회사의 물리적 보안실천에 대하여서는 발언권이 없을수 있다. 그러나 그는 자기 망을 엿듣는것이 조금이라도 어렵게 되도록 하기 위하여 노력하여야 한다.

물리적매체를 선택할 때 다른 보안조치들이 좀 약하다면 망이 공격에 더 잘 견디도록 하여야 한다는것을 명심하여야 한다.

중추망로막들이 접근가능한가

공격자가 망을 감시하려고 하고 있다면 그는 대부분의 정보를 모을수 있는 중심마디를 찾으려고 할것이다. 배선실과 봉사기실은 많은 통신대화들을 접속시켜 주는 구역이므로 가장 좋은 목표로 된다. 망을 배선할 때 이 지역들에 특별한 주의를 돌리며 가능하면 보다 안전한 매체(빛섬유와 같은)의 사용을 고려하여야 한다.

자료전송방법을 선택할 때 이 문제들을 주의 깊게 고찰하여야 한다. 제2장에서 본 위험분석정보를 리용하여 자기의 선택을 증명하여야 한다. 위상구조적인 보안의 수준을 높이는것은 매우 비용이 드는것으로 보일수 있는데 그 비용은 침입으로부터의 회복비용과 비교할 때 증명된것보다 더 많을수도 있다.

위상구조적인 보안

자료를 나르는데 준비된 전송매체에 대한 리해에 기초하여 이 매체들이 하나의 망으로서 기능하기 위하여 어떻게 구성되는가를 고찰하기로 한다. 위상구조는 주어 진 망 매체우에서 물리적으로 련결하고 통신하기 위한 규칙들로서 정의된다. 매개 위상구조는 망체계들을 련결하기 위한 자기의 규칙모임을 가지며 어떻게 이 체계들이 배선우에서 서로 《말해야》 하는가를 규정하고 있다. 지금까지 가장 널리 쓰이는 국부망위상구조는 이써네트이다.

이써네트

제3장에서 우리는 이써네트프레임에 어떤 형식의 정보가 포함되는가를 보았다. 이제는 이써네트가 어떻게 이 정보를 망을 통하여 한 체계로부터 다른 체계에로 이동하는가를 시험해 보기로 한다. 망통신특성들을 더 잘 알고 있을수록 망을 안전하게 하기가 더 쉬울것이다.

주 의

이써네트는 1970년대 말에 Xerox에 의하여 개발되였다. 그것은 후에 IEEE 802.3으로 발전하였다. 그것의 유연성, 높은 전송속도 그리고 비독점적인 특성으로 하여 인차 많은 망관리자들이 선택하는 망위상구조로 되였다.

이써네트는 지금까지 가장 대중적인 망위상구조이다. 여러가지 형태의 케블을 지원하는 능력, 낮은 가격의 장치구조 그리고 PnP련결성 등으로 하여 그것은 그 어떤 다른 위상구조보다 좋은 기업망(또는 가정망)으로 인정되게 되였다.

이써네트의 통신규칙은 충돌검출을 가진 반송파수감다중접근(CSMA/CD)이라고 부른다. 이것은 발음하기 어려운 긴 말이기는 하지만 그것을 분석하면 리해하기 쉽다.

- 반송파수감이란 이써네트국들이 모든 시간동안(지어 전송하고 있을 때에도) 모선상에서 들어야 한다는것을 의미한다. 《듣는다》는것은 그 국이 망을 계속 감시하면서 어떤 다른 국이 현재 자료를 전송하는가 하는것을 알아 내는 것을 의미한다. 다른 국의 전송을 감시함으로써 국은 망이 열려 있는가 리용중에 있는가를 알수 있다. 이 방법에서 국들은 맹목적으로 정보를 전송하여 다른 국들을 방해하지 않는다. 부단한 듣기방식에 있다는것은 그 국이 다른 국이 자료를 전송하려고 할 때 준비되여 있다는것을 의미한다.
- 다중접근은 간단히 두개이상의 국이 같은 망에 련결될수 있다는것 그리고 망이 자유로와 질 때마다 모든 국이 전송할수 있다는것을 의미한다. 매 체계가 지정된 시간에 전송하는것보다 그들이 요구하는 때에 전송할수 있는것은 매우 효과적이다. 다중접근은 또한 망에 더 많은 국들을 추가할 때 그것을 쉽게 확장할수 있게 한다.
- 충돌검출은 다음의 물음에 대답한다.《두 체계가 회선이 자유롭다고 생각하고 동시에 자료를 전송하려고 한다면 무슨 일이 일어 나겠는가?》 두개의 국이 동시에 전송하면 충돌이 발생한다. 충돌은 간섭과 류사한데 결과적인 전송은 실패하고 자료를 나를수 없게 된다. 한 국이 자료를 전송할 때 그것은 이 조건을 감시한다. 만일 이러한 조건을 검출한다면 그 워크스테이션은 충돌이 일어 났다고 가정한다. 그 국은 다시 들어 가서 우연시간만큼 기다렸다가 다시 전송한다.

주　　의

매개 국은 재전송하기전에 자기의 우연대기시간을 결정하여야 한다. 이렇게 하여야 매개 국이 서로 다른 시간동안 기다리며 또 다른 충돌을 피할수 있게 된다. 두번째 충돌이 발생하면(그 국이 들어 갔다가 다시 나와 충돌한다.) 매개 국이 기다리는 동작을 또 반복하여야 한다. 둘 또는 그이상의 련속적인 충돌이 발생하면 그것을 다중충돌이라고 부른다.

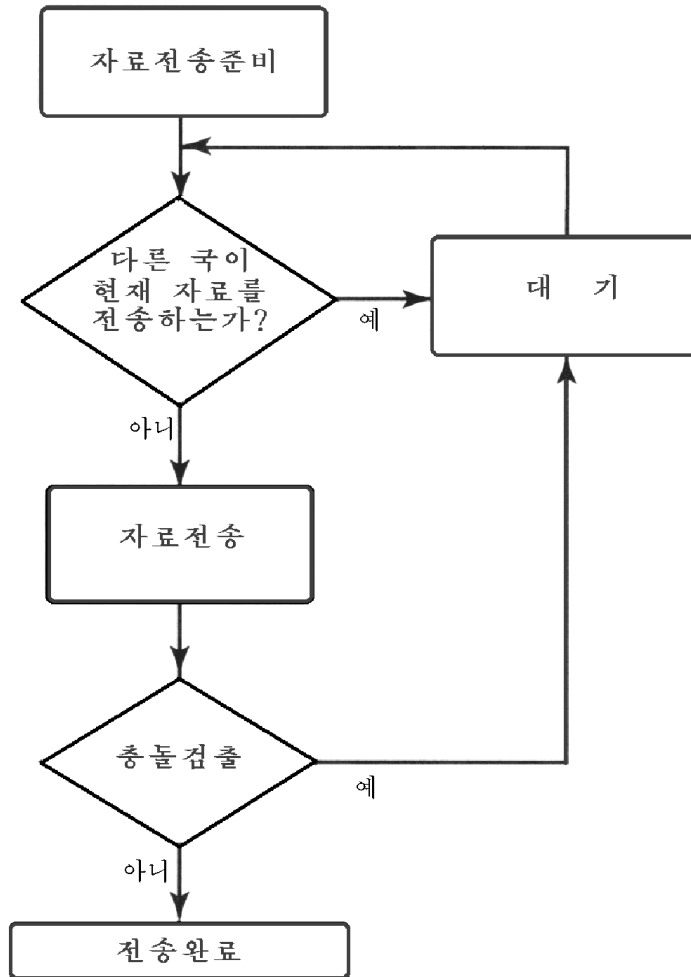



그림 4-5. 이써네트통신규칙의 흐름도

CSMA/CD의 동작을 그림 4-5에 보여 주었다. 이 과정은 제3장에서 고찰한 ARP결정과정후에 일어 나는 과정이다.

무차별방식

이써네트통신에서 절대적으로 필요한 부분은 매 체계가 다른 모든 국들의 전송을 부단히 감시하고 있다는것이다. 그런데 이것은 또한 이써네트의 가장 큰 보안약점으로 된

다. 한 체계가 수신하는 이 모든 정보를 읽을수 있도록 체계를 구성하는것이 가능하다. 이것을 보통 무차별방식체계라고 부른다.

무차별방식은 망관리자가 하나의 중심국으로부터 망을 감시하여 오유들과 망통계자료들을 모을수 있게 함으로써 개선될수 있다. 망분석기는 무차별방식에서 효과적으로 동작하는 하나의 콤퓨터이다. 하나의 국이 모든 망자료흐름들을 듣고 있으므로 간단한 쏘프트웨어의 변화로서 체계가 모든 정보들을 기록하게 할수 있다.

그런데 무차별방식의 존재는 또한 그리 정직하지 못한 사람이 망통신을 엿듣거나 민감한 정보들을 훔칠 가능성이 있다는것도 말하고 있다. 이것은 콤퓨터망을 통과하는 대부분의 정보가 평문형태로 되여 있는것으로 하여 특별히 문제로 된다. 그림 4-6에 이러한 하나의 실례를 보여 준다.

망감시자가 또는 망분석기가 수집할수 있는 정보의 크기를 최소화하기 위하여서는 망자료흐름들을 고립된 망통신들로 토막내야 한다. 이것은 망다리, 교환기 또는 경로기들을 리용하면 가장 잘 수행할수 있다. 이 장치들은 이 장의 《기초적인 망련결장치》에서 고찰된다.

```
Packet Number : 13          3:52:02 PM
Length : 66 bytes
ether: ===================== Ethernet Datalink Layer =====================
        Station: Skylar ----> This_Workstation
        Type: 0x0800 (IP)
    ip: ======================== Internet Protocol ========================
        Station:10.1.1.180 ---->10.1.1.25
        Protocol: TCP
        Version: 4
        Header Length (32 bit words): 5
        Precedence: Routine
                Normal Delay, Normal Throughput, Normal Reliability
        Total length: 40
        Identification: 21249
        Fragmentation not allowed, Last fragment
        Fragment Offset: 0
        Time to Live: 128 seconds
        Checksum: 0x9148(Valid)
   tcp: ================= Transmission Control Protocol =================
        Source Port: 258
        Destination Port: 1027
        Sequence Number: 417610
        Acknowledgement Number: 898472
        Data Offset (32-bit words): 5
        Window: 8518
        Control Bits: Acknowledgement Field is Valid (ACK)
                Push Function Requested (PSH)
        Checksum: 0x5DB5(Valid)
        Urgent Pointer: 0
```

그림 4-6. 하나의 망파일의 파케트내용

광지역망위상구조

광지역망(WAN)위상구조는 넓은 지역을 통하여 자료를 전송하도록 설계된 망구조이다. 많은 체계들사이에서 자료를 배포하도록 설계된 LAN과 달리 WAN는 보통 점대점으로 동작한다. 점대점(Point to Point)이란 위상구조가 자료를 보내고 받는 두 마디점만을 지원하도록 개발된 기술을 의미한다. 만일 여러개의 마디점이 그 WAN에 접근하려고 한다면 LAN은 그 뒤에 위치하여 이 기능을 수행하게 된다.

전용회선 위상구조

임대선이란 고정료금지불에 기초한 전용의 상사 또는 수자회선이다. 이것은 그 회선

을 리용하든 안하든 관계없이 달마다 고정된 료금을 물고 있다는것을 의미한다. 임대선은 점대점련결로서 한 지리적위치를 다른 지리적위치에 련결하는데 리용된다. 임대선의 최대 처리량은 56Kbps이다.

T1은 두쌍의 도선케블에 의한 전2중련결회선(련결의 매 끝은 동시에 전송하고 수신할수 있다.)이다. T1들은 임대선과 같이 전용 점대점련결을 위하여 쓰인다. T1에서 대역너비는 64KB로부터 1.544MB까지 준비되여 있다. T1는 시분할방법으로 두 도선쌍을 24개의 개별적인 통로들로 쪼갠다. 시간분할이란 준비되여 있는 대역너비를 시간증분에 기초하여 할당하는것이다. 이것은 T1이 음성과 자료를 동시에 나를수 있게 하므로 매우 유용하다.

임대선이나 T1들을 배비하는데 두가지 공통적인 방법이 있다.

- 회선이 두 시설사이의 련결의 전체 길이를 구성한다(분사무소와 기본사무소와 같은).
- 임대선은 매 위치로부터 그것의 국부적교환설비까지의 련결을 위하여 리용된다. 그리고 두 교환설비들사이의 련결은 프레임중계와 같은 어떤 다른 기술에 의하여 제공된다(이것은 다음 절에서 취급한다).

이 두가지 선택중 첫째가 보다 안전한 련결을 만드는데 비용은 보다 비싸다. 두개의 지리적으로 떨어 진 장소들사이에서 점대점련결을 위하여 전용회선을 리용하는것은 자료가 감시되지 않도록 담보하는 가장 좋은 방법이다. 이 회선들중 하나를 《냄새 맡는것》은 아직 가능하지만 공격자는 그것의 경로를 따라 어떤 점에 물리적으로 접근하여야 한다. 또한 공격자는 감시하려는 특정의 회선을 식별할수 있어야 한다. 전화반송기나 써서는 공격자가 좋아 하는 문장인 《은행 XYZ의 금융자료, 여기서 감시할것》과 같은것을 얻을수 없다.

두번째 선택은 보통 국부적교환설비에로의 신호를 얻는데 리용된다. 거기로부터 자료는 프레임중계나 X.25와 같은 공공망으로 나가게 된다.

프레임중계와 X.25

프레임중계와 X.25는 파케트교환기술이다. 파케트교환망에서 자료는 어떤 준비된 회선경로를 따라 갈수 있으므로 이러한 망들은 그림 4-7과 같은 그라프적표현에서 흐린색으로 표시된다.

X.25와 프레임중계는 둘 다 영구가상회선(PVC)으로 구성되여야 하는데 이것은 점 A에서 흐림구역안으로 들어 가는 모든 자료는 자동적으로 점 B로 전송된다는것을 의미한다. 이 끝점들은 봉사가 시작되는 시점에서 정의된다. 큰 WAN환경에서 프레임중계는 전용회선보다 매우 비용이 클수 있다. 이것은 하나의 WAN련결을 통하여 여러개의 PVC들을 돌릴수 있기때문이다.

실례로 어떤 사람이 집사무실까지 56KB의 련결을 요구하는 4개의 원격싸이트들을 가지고 있다고 하자. 만일 그가 이 망을 전용회선없이 구축하였다면 매개의 원격싸이트에서 하나의 56KB 임대선련결을 만들고 또한 기본사무소에로 가는 4개의 56KB 임대선련결을 만들었을것이다.

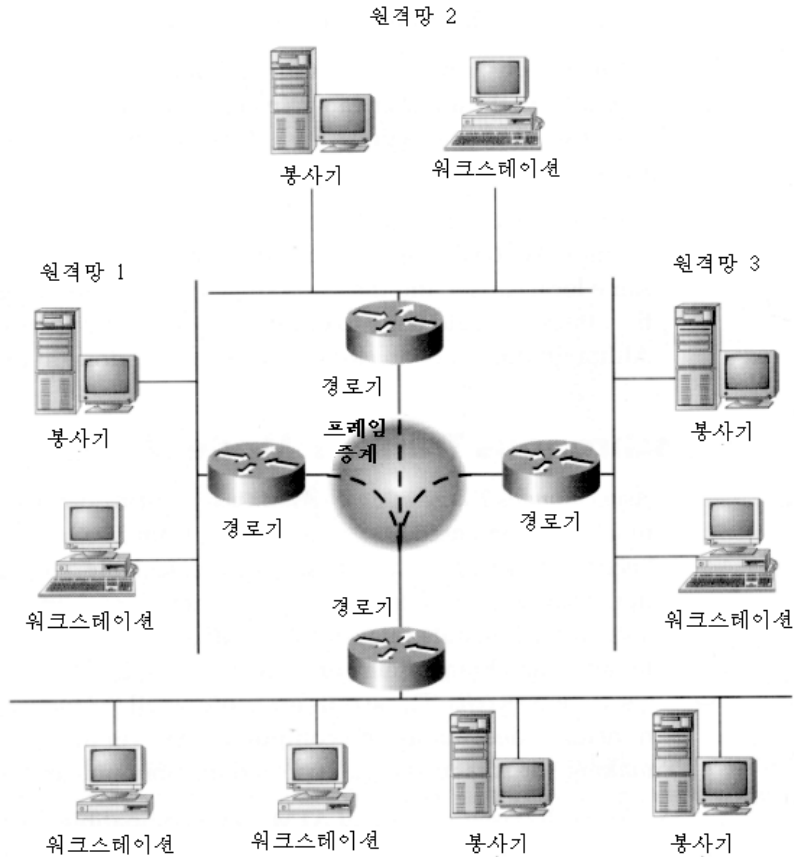



그림 4-7. 3개의 원격망들을 하나의 기업사무소에 련결하는
WAN프레임중계기

그러나 프레임중계를 리용하면 기본사무소에서의 4개의 전용련결을 하나의 기능적인 T1련결로 바꾸고 T1회선의 4개 통로를 자료를 받아 들이도록 동작시키면 된다. 기본싸이트에서 하나의 회선망을 리용함으로써 그것은 WAN비용을 줄일수 있다.

사실상 기본사무소에서의 CIR가 그의 모든 원격싸이트들의 CIR값과 같아야 한다는 것은 없다. 실례로 그의 원격싸이트에로의 련결이 엄격히 전자우편을 전송하기 위하여 리용된다고 가정하자. 대역너비요구가 낮다면 기본사무소에서 CIR를 256KB로부터 128KB로 낮출수 있다. 그것의 4개의 원격싸이트들에로의 전체 통신량이 128KB를 초과하지 않는 한 그것은 성능이 떨어 졌다는것을 알아 차리지 못할것이다. 이것은 WAN비용을 크게 감소시킬것이다.

주 의

파케트교환망은 공유매체이다. 교환설비는 그것이 임대하는 모든 PVC들을 위하여 같은 망을 리용한다. 결과적으로 매 다른 의뢰기들과 준비되여 있는 대역너비를 공유하고 있다.

흐림구역에로의 련결점은 자료련결층련결식별자(DLCI)를 리용하여 배당된다. DLCI는 국부적교환설비로 하여금 그것이 어느 PVC를 련결에 넘기기하여야 하는가를 알도록 한다.

매개가 자기의 지정된 DLCI를 사용하는 한 문제가 생기지 않는다. 문제는 어떤 사람이 부정확하게 또는 나쁜 의도에서 자기의 경로기를 남의 회선과 같은 DLCI로 지정하였을 때 생긴다. 이것은 자료흐름이 그들의 망에로 들어 가게 할수 있다. 이렇게 되려면 다음의 조건들이 성립하여야 한다.

1. 공격자가 같은 국부적교환설비에 련결되여야 한다.
2. 공격자가 같은 물리적교환기에 련결되여야 한다.
3. 공격자가 남의 DLCI를 알아야 한다.

명백히 이것은 실현하기에 가장 어려운 공격은 아니다. 그것은 비용이 드는 일이지만(공격자가 다른 기관의 망에 접근할수 없고 그 련결을 《빌릴수》 없는 한) 공격자가 그 련결로 중요한 정보가 통과하고 있다는것을 안다면 이 공격은 노력해 볼만 한 가치가 있는것이다.

또한 공격자는 또 다른 지리적위치에로 하나의 PVC를 돌릴수 있다. 그렇게 하는것은 자료를 얻기 위하여 같은 국부설비나 같은 교환기를 통하여 련결되는 필요성을 제거하는것으로 되며 또한 공격자가 교환설비관리체계에 침투하여야 한다는것을 의미한다. 이것은 쉬운 문제가 아니지만 지난 시기에 실행되였었다.

비동기전송방식(ATM)

비동기전송방식(ATM)은 25-622Mbps의 속도범위에서 가장 널리 실현된 점대점 WAN 기술이다. ATM은 전송의 임대선에 비하여 효과적인 비용, 확대가능한것, 믿음성이 높은것 등으로 하여 널리 퍼졌으나 역시 사용자인증, 자료완전성, 자료유효성, 자료비밀성 등을 론의할 때는 중요한 취약점들을 가지고 있다. ATM은 프레임중계나 X.25와 다르게 동작하는데 그것은 자료를 세포(cell)라고 부르는 고정크기의 파케트로 쪼갠다. 이 세포들은 매우 작은데(53byte) 그것으로 하여 같은 망을 통하여 영상, 음성 그리고 콤퓨터자료들을 전송할수 있게 하며 하나의 자료형식이 대역너비를 독점하지 못하도록 한다.

ATM의 세포파케트들은 파케트려과방화벽과 호환되지 않는다. 왜냐하면 이 방화벽들은 점대점 ATM련결의 끝점으로 간주되여야 하기때문이다. ATM파케트의 토막화 및 재조립(SAR)의 부차적지출은 효과적인것으로 되지 않는다. 또한 ATM봉사들은 비IP자료흐름을 전송할수 있으므로 IP자료흐름과 결합되지 않는 약점들이 있다(그리고 그로 하여 전통적인 IP망보안구조를 적용할수 없다.).

그러면 해커는 어떻게 ATM자료에 접근할수 있겠는가? 첫번째 방법은 전송매체와 관계된다. 이것은 반드시 해커를 제지하는것으로는 되지 못한다. 해커는 빛섬유의 절연을 떼고 그것을 구부려 전송통로의 빛을 밖으로 나오게 하여 엿듣는다(그러나 대화가 끊어 져서 경보가 울리지는 않게끔 한다.).

두번째 방법은 망에서 돌아 가는 가상회선의 우점을 리용한다. 즉 교환가상회선(SVC) 또는 영구가상회선(PVC)을 리용한다. 대부분의 SVC관리체계는 《호출에 더하

기》라는 특성을 가지는데 이것은 임의의 체계가 현재 집행중의 대화에 참가할수 있게 한다. 만일 SVC관리자가 하나의 대화를 미리 정의하지 않고 닫지 않았다면 임의의 사람이 거기에 참가하고 엿들을수 있다. PVC도 관리체계에서는 취약한데 특히 그들의 대면부가 telnet나 Web에 기초하고 있다면 해커는 통과암호를 《냄새》 맡거나(telnet의 경우에) 또는 실현상의 약점을 리용(Web에 기초한 도구)할수 있다.

일단 해커가 망에 접근을 하였다면(그리고 자기 소유의 PVC 또는 SVC를 만들수 있다면) 그들은 잠정국부관리대면부(ILMI) 또는 전용망대망대면부(PNNI)를 리용하여 ATM망의 경로정보를 변화시키며 자료를 정확히 자기들이 관리하는 인터네트상의 한 체계에로 보낼수 있다.

기초적인 망련결하드웨어

지금 자기의 망하부구조를 계획할 때 구할수 있는 망제품은 매우 많다. 콤퓨터체계를 망에 련결하며 망자료흐름을 조종하기 위하여 위상구조명세를 확장하기 위한 모든 장치들이 있다. 때로 그 선택은 제한된다. 실례로 하나의 사무실콤퓨터를 망에 련결하기 위하여서는 망기판이 있어야 한다.

이러한 많은 장치들은 정확히 리용된다면 망의 보안을 개선하는데도 도움이 될수 있다. 이 절에서 우리는 일부 공통적인 망장치들을 살펴 보고 보안자세를 강화하기 위하여 어느것을 쓸수 있겠는가를 론의할것이다.

반복기(Repeater)

반복기는 간단한 두 포구신호증폭기이다. 이것들은 모선형위상구조에서 하나의 케블로 나갈수 있는 최대거리를 늘이기 위하여 리용된다. 신호의 세기는 그것이 도선을 따라 전파되는데 따라 보강된다. 반복기는 한 포구로 수자식신호를 받아서 그것을 증폭하여 다른쪽 포구로 전송한다.

반복기는 전형적인 가정용립체증폭기와 류사하다. 증폭기는 CD나 테프로부터 받은 신호를 증폭하고 그것을 고성기로 가는 길로 내보낸다.

반복기가 수신한 신호는 좋은 자료프레임, 나쁜 자료프레임 또는 배경잡음일수도 있다. 반복기는 자료의 질을 식별하지 않고 그것들을 그대로 증폭한다.

반복기는 자료토막화를 하지 않는다. 반복기의 한쪽에서 발생하는 모든 통신은 수신체계가 도선의 다른쪽에 있던 아니던 관계없이 반복기의 다른쪽으로 통과된다. 반복기를 피동적인 증폭기로 생각하면 된다.

집선기(Hub)

집선기는 아마 망대면부기판에 다음 가는 가장 널리 쓰이는 망장치라고 볼수 있다. 물리적으로 집선기는 여러개의 RJ45암접속구를 가지는 변하는 크기의 통이다. 매개 접속구는 RJ45수접속구를 붙인 하나의 꼬임쌍선케블을 꽂도록 설계되였다. 그

러면 이 꼬임쌍선케블은 하나의 봉사기 또는 워크스테이션을 집선기에 련결하는데 리용된다.

집선기는 본질에 있어서 별형위상구조에서 꼬임쌍선케블을 지원하는 여러포구반복기이다. 매 마디점들은 집선기와 통신하며 집선기는 그 신호들을 증폭하고 그것들을 매개 포구들에로(전송하는 체계도 포함하여) 전송한다. 반복기와 마찬가지로 집선기도 전기적준위에서 동작한다. 집선기는 자료흐름조종을 제공하지 않으며 기능적으로 반복기와 같다.

무선집선기

전통적인 집선기의 한가지 변종은 무선집선기이다. 이 집선기들은 꼬임쌍선대신에 무선전송을 리용하는데 무선NIC를 가진 콤퓨터들이 이 집선기를 통하여 서로 통신하게 된다. 보안문제와 관련하여서는 대부분의 무선집선기제작자들은 무선체계에서 기본적으로 암호화를 리용하고 있다.

망다리(Bridge)

망다리는 반복기와 비슷하게 생겼는데 망의 두개의 분리된 부분에 속하는 두개의 망접속구를 가지는 작은 통이다. 망다리는 반복기의 기능(신호증폭)을 포함하지만 사실상 자료프레임을 취급하며 이것이 큰 우점이다. 그림 4-8에 보여 준것처럼 일반적인 망다리는 지시등을 제외하고는 반복기와 거의 비슷하게 생겼다. 《Forward》지시등은 망다리가 한 충돌령역으로부터 다른 곳으로 자료흐름을 통과시켜야 할 때 불이 켜진다.

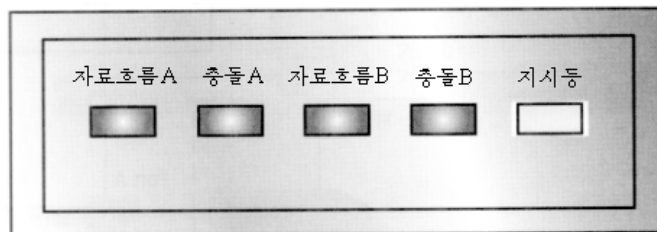



그림 4-8. 일반적인 망다리

제3장의 이써네트에 대한 고찰에서는 자료프레임에 대한 개념을 소개하고 프레임머리부안에 포함된 정보들을 서술하였다. 망다리는 매 자료프레임에서 머리부정보를 리용하여 원천 및 목적지 MAC주소를 감시한다.

원천주소로부터 망다리는 그 망체계가 어디에 위치하고 있는가를 알게 된다. 망다리는 하나의 표를 만드는데 자기의 매 포구에 의하여 어느 MAC주소로 직접 접근가능한가를 목록으로 만든다. 그리고 이 정보를 리용하여 교통정리원역할을 하며 망에서 자료와 흐름을 조절한다. 하나의 실례를 보자.

망다리실례

그림 4-9의 망을 고찰하자. Betty는 자료를 봉사기 Thoth에게 보내려고 한다. 망우의 매개가 다 망을 감시하여야 하므로 Betty는 먼저 다른 국들이 전송을 하는가를 듣는다. 도선이 비였다면 Betty는 하나의 자료프레임을 전송한다.

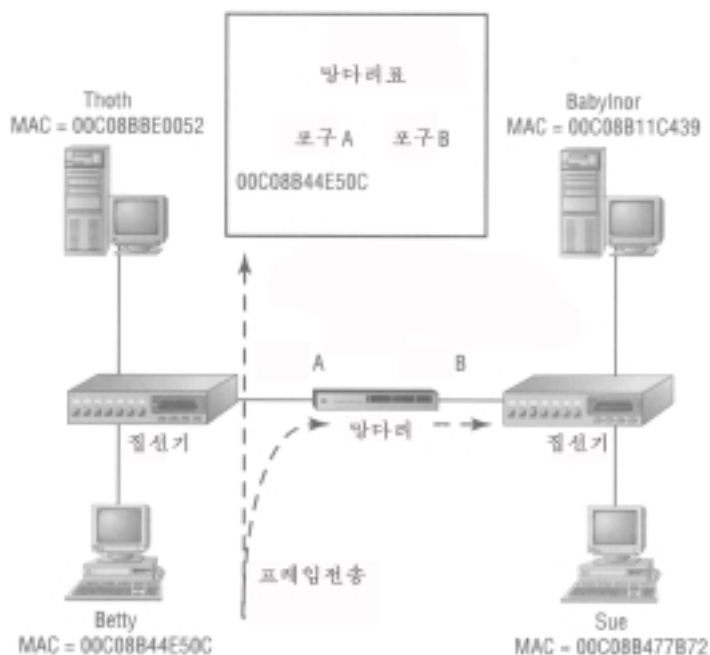



그림 4-9. Betty가 자료를 봉사기 Thoth에게 전송한다. Thoth의 MAC 주소는 프레임머리부의 목적지마당에 들어 있다

망다리도 또한 자료흐름을 감시하고 있다가 Betty의 프레임의 머리부에서 목적지주소를 본다. 망다리는 MAC주소 00C08BE0052(Thoth)를 가지는 체계가 어느 포구에 련결되여 있는지 모르므로 그 신호를 증폭하여 포구 B로 재전송한다. 지금 망다리의 기능은 반복기와 류사하다. 그러나 약간의 일을 더하는데 그는 Betty가 포구 A에 붙어 있다는것을 알고 그의 MAC주소를 가지는 하나의 표항목을 만든다.

그림 4-10에서 보여 준것처럼 Thoth가 Betty의 요청에 응답할 때 망다리는 자료프레임에서 목적지주소를 또 보게 될것이다. 그러나 이때 그는 그것을 자기의 표와 맞추어 보고 Betty가 포구 A에 붙어 있다는것을 알게 된다. 그는 Betty가 이 정보를 직접 받을수 있다는것을 알고 있으므로 그 프레임을 떨구고 포구 B로부터 전송되지 않도록 막는다. 망다리는 또한 Thoth에 대한 새로운 표항목을 만들어 그 MAC주소가 포구 A에 있는것으로 기록한다.

망다리가 매 국의 MAC주소를 기억하고 있는 한 Betty와 Thoth사이의 모든 통신은 Sue와 Babylnor와는 차단될것이다. 자료흐름의 격리는 망다리의 량쪽에 있는 체계들이 준비되여 있는 대역너비를 2중으로 쓰면서 효과적으로 동시에 대화를 진행한다는것을 의

미하므로 매우 강력한 기능으로 된다. 망다리는 그 량쪽이 서로 련결되지 않은것처럼 통신이 격리되도록 담보한다. 국들은 망다리의 다른쪽에서의 전송을 볼수 없으므로 자기들의 망이 현재 비여 있다고 가정하고 자기들의 자료를 전송하게 된다.

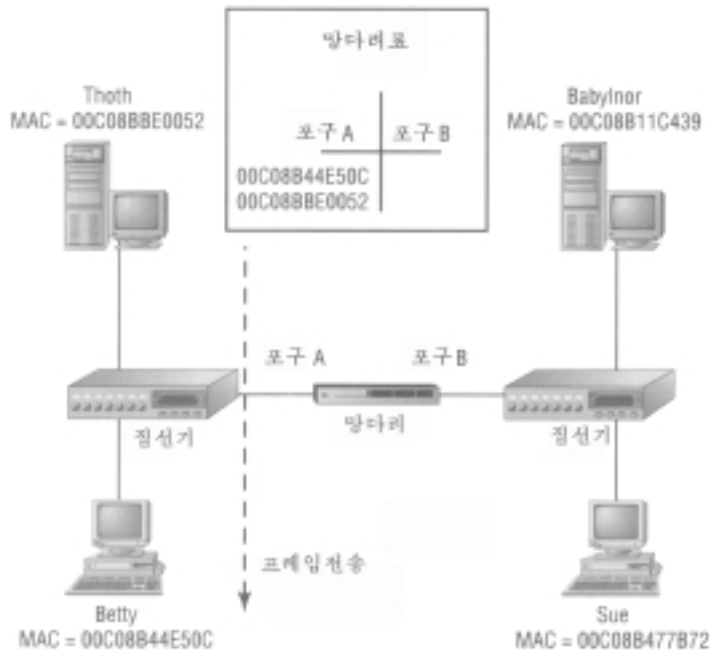



그림 4-10. Thoth가 Betty의 통보문에 응답한다

매개 체계는 자기와 같은 망토막에 있는 체계들과만 대역너비를 가지고 다투게 된다. 이것은 그 토막밖에서는 충돌이 생길수 없다는것을 의미한다. 그러므로 이 토막들은 그림 4-11에 보여 준것처럼 충돌령역이라고 부른다. 망다리의 매 측에서의 하나의 포구는 매 충돌령역의 부분으로 된다. 그것은 그의 매 포구들이 그것에 직접 접속된 체계들과 대역너비를 가지고 다툴것이기때문이다. 망다리는 매 충돌령역안에서 통신량을 격리시키므로 분리된 체계들이 충돌할수는 없다. 그 효과는 잠재적인 대역너비를 2배로 하는것으로 나타난다.

망을 두개의 충돌령역으로 분리하는것은 망보안을 강화하는것으로 된다. 실례로 Babylnor라는 체계가 손상되였다고 하자. 공격자는 이 체계에 높은 급의 접근을 얻고 중요한 정보들을 구하기 위하여 망활동을 포착하기 시작한다.

우의 망설계가 주어 졌다고 하면 Thoth와 Betty는 비교적 안전하게 대화를 할수 있다. Babylour의 충돌령역으로 갈수 있는 유일한 자료흐름은 방송자료뿐이다. 제3장에서 방송프레임은 모든 국부체계에 배달된다는것을 보았다. 그러므로 망다리는 방송자료흐름을 전송할것이다.

이러한 상태에서 망다리를 리용하면 2중으로 상금을 타는것과 같다. 성능이 높아 질뿐만아니라 보안도 강화된다.

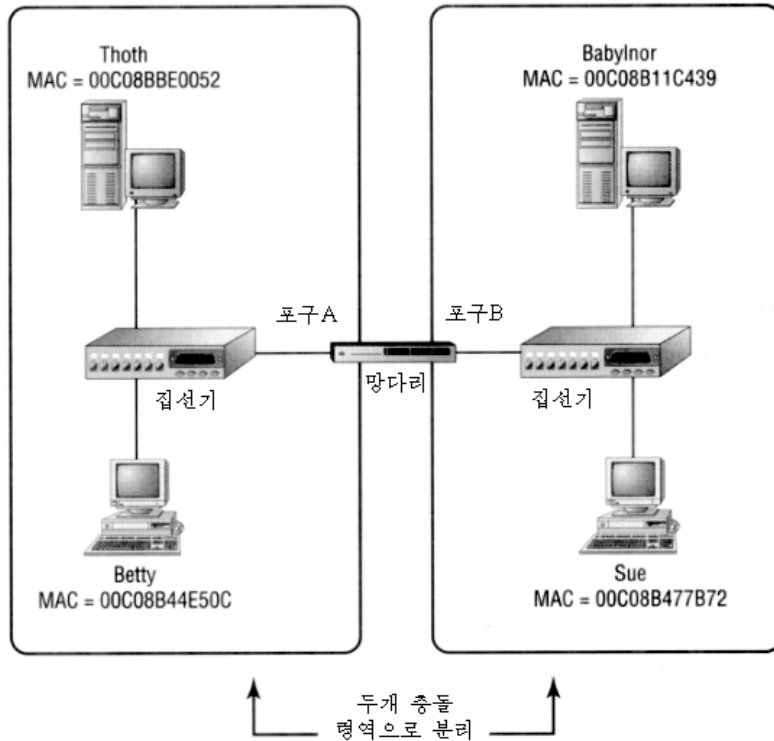



그림 4-11. 두개의 분리된 충돌령역

그러면 자료흐름이 망다리를 통과할 때 무슨일이 생기게 되는가? 언급된바와 같이 망다리는 체계의 위치를 모를 때 그 파케트를 그대로 통과시킨다. 일단 망다리는 그 체계가 사실상 다른 포구에 위치하고 있다는것을 알면 그 프레임을 요구하는대로 통과시킨다.

실례로 만일 Betty가 Sue와 통신하기 시작한다면 이 자료는 망다리를 지나서 Babylnor와 같은 충돌구역으로 전송될것이다. 이것은 Babylnor가 이 자료를 받을수 있다는것을 의미한다. 망다리는 Betty와 Thoth의 통신은 안전하게 보장하였지만 Betty가 Sue와 통신하기 시작할 때에는 추가적인 보안을 제공하지 못한다.

이 대화들을 둘다 안전하게 하기 위하여서는 망다리가 매개 체계에 하나의 포구를 제공할수 있어야 한다. 이러한 형식의 기능은 교환기라고 부르는 장치에 의하여 제공된다.

교환기

교환기는 집선기와 망다리기술의 결합이라고 볼수 있다. 이것들은 겉으로 보기에는 집선기와 류사한데 망체계들을 접속하기 위한 여러개의 RJ45접속구들을 가지고 있다. 그러나 집선기와 같은 피동적인 증폭기가 아니라 교환기는 매 포구에 작은 망다리를 가지고 있는것처럼 동작한다. 교환기는 매 포구에 붙은 MAC주소들의 위치를 알고 있으며 일정한 주소에로 정해 진 자료흐름을 그것이 속한 포구에로만 보낸다.

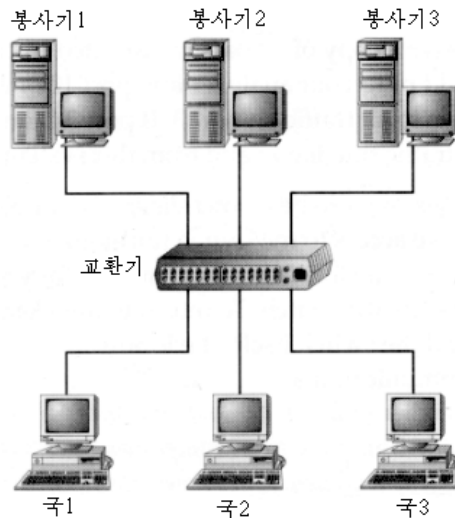



그림 4-12. 통신하려고 하는 3개의 국과 3개의 봉사기를
보여 주는 교환기설치환경

그림 4-12는 매개 장치가 자기의 전용포구에 접속된 교환기에 기초한 환경을 보여준다. 교환기는 하나의 프레임전송이 발생하면(망다리와 같이) 그 국의 MAC식별자를 배운다. 이것이 이미 진행되였다고 가정하면 정확히 같은 순간에 국 1은 봉사기 1에 자료를 보내려 하고 국 2는 봉사기 2에 자료를 보내려 하며 국 3은 봉사기 3에 자료를 보내려 한다는것을 알게 될것이다.

이 정황과 관련하여 몇가지 흥미 있는것들이 있다. 첫째로는 매 도선의 동작이 그 교환기와 그것에 붙은 그 국만을 포함한다는것이다. 이것은 매개 충돌령역이 이 두 장치만에로 제한되였다는것을 의미한다. 왜냐하면 교환기의 매개 포구는 망다리와 같이 동작하기때문이다. 워크스테이션과 봉사기가 보는 유일한 자료흐름은 특별히 그들에게로 보내진 프레임과 방송주소로 보낸것들뿐이다. 결과로 3개의 모든 국들은 매우 작은 망자료흐름을 보게 되며 즉시로 전송할수 있게 된다. 이것은 잠재적인 대역너비를 크게 증가시키는 좋은 특성으로 된다. 우의 실례에서 이것이 10Mbps위상구조라면 결과적인 처리량은 3배로 증가할것이다. 이것은 3개의 체계모임전체가 교환기에 의하여 격리되여 있으므로 동시에 대화를 할수 있기때문이다. 기술적으로는 10Mbps이써네트이지만 잠재적인 처리량은 30Mbps로 증가하였다.

성능을 크게 높이는 한편 보안도 강화되게 된다. 이 체계들중 어느 하나가 손상되면 감시될수 있는 유일한 대화는 손상된 체계와의 대화뿐이다. 실례로 만일 공격자가 봉사기 2에로의 접근을 얻었다면 그는 봉사기 1 또는 3과의 통신대화는 감시할수 없을것이다.

이것은 감시하는 장치가 자기의 충돌령역안에서 전송하는 자료흐름만을 모을수 있기때문이다. 봉사기 2의 충돌령역은 그 자체와 그것이 접속된 교환기포구로 구성되여 있으므로 교환기는 다른 봉사기들과 진행되는 통신대화로부터 봉사기 2로 격리하는 작업을 효과적으로 수행한다.

이것은 훌륭한 보안특성이지만 망에 대한 합법적인 감시는 좀 시끄러운 일로 된다.

이것으로 하여 많은 교환기들은 감시포구를 가지고 있다.

감시포구는 그 교환기의 하나의 포구로서 하나 또는 몇개의 포구들에로 전송된 모든 자료들의 복사들을 수신하도록 구성될수 있다. 실례로 자기의 분석기를 교환기의 포구 10에 꽂고 그 장치가 포구 3에로의 모든 자료흐름을 듣게끔 구성할수 있다. 만일 포구 3이 자기의 봉사기들중 하나라면 지금 이 체계에로 들어 오고 나가는 모든 자료흐름을 분석할수 있다.

이것은 또한 잠재적인 보안구멍일수도 있다. 만일 공격자가 그 교환기에로의 관리접근을 얻을수 있다면(telnet, HTTP, SNMP 또는 조종탁도구를 통하여) 그는 그 교환기에 접속된 임의의 체계 또는 그것을 통하여 통신하는 임의의 체계를 감시하는데서 자유로운 통제권을 가지게 될것이다. 우의 실례에로 돌아가서 만일 공격자가 봉사기 2와 교환기자체에 접근할수 있다면 그는 지금 모든 망통신을 완전히 감시할수 있게 된다.

주 의

망다리, 교환기 그리고 류사한 다른 망장치들은 주로 보안을 개선하기 위해서가 아니라 망성능을 개선하기 위하여 설계된것들이다. 보안이 강화되는것은 두번째의 유익한 점이다. 이것은 그것들이 방화벽이나 경로기와 같이 《마구다루기식》의 현실세계체험을 겪어 보지 못하였다는것을 의미한다. 교환기는 보안방책을 좋게 하여주지만 그것이 보안방책을 실현하는데서 핵심적인 장치로 되여서는 안된다.

VLAN 기술

교환은 가상국부망(VLAN)이라고 하는 새로운 기술을 도입한다. 교환기에서 돌아가는 쏘프트웨어는 지리적위치에 의해서가 아니라 작업집단에 의하여 련결된(VLAN집단이라고 부르는) 체계들의 련결성파라메터들을 설정할수 있게 한다. 교환기의 관리자는 포구전송을 론리적으로 조직하여 련결성이 매 사용자의 요구에 따라 집단을 짓도록 할수 있다. 《가상적인》부분은 이 VLAN집단들이 여러개의 물리적망토막들과 여러개의 교환기들을 포함할수 있다는것이다. 일정한 집단의 사람들이 PC에 접속된 모든 교환기포구들을 같은 VLAN집단에 배당함으로써 하나의 가상적인 망을 만들수 있다.

VLAN을 여러개의 교환기를 만들기 위하여 많은 포구를 가지고 있는 하나의 교환기를 쪼개여 쓰는것의 가상적인 등가물로 생각하면 된다. 만일 하나의 24포구교환기를 가지고 있고 그 포구들을 나누어 3개의 꼭 같은 VLAN을 만들려고 한다면 이것은 본질에 있어서 3개의 8포구교환기를 가지고 있는것과 같다. 여기서 《본질에 있어서》라는 말이 아주 중요한데 그것은 사실 하나의 물리적장치를 가지고 있기때문이다. 이것은 관리를 보다 간단하게 해주지만 보안의 견지에서 보면 3개의 물리적인 교환기를 가지는것만큼은 좋지 못하다. 만일 공격자가 VLAN을 리용하여 교환기를 손상시킬수 있다면 그는 그 장치우에 있는 다른 VLAN들을 감시할수 있도록 자기의 련결을 구성할수 있게 된다.

이것은 방화벽과 같은 자료흐름조종장치의 량쪽에 련결을 제공하는 하나의 큰 교환기를 가지고 있는 경우에 매우 나쁜것으로 된다. 공격자는 방화벽에 침투할 필요가 없을수도 있다. 그는 교환기가 훨씬 더 쉬운 목표라는것을 알게 될것이다. 적어도 공격자는 지금 망에 침투할 두가지의 잠재적인 길을 알고 있는것으로 된다.

경로기

경로기는 통신규약과 망정보에 기초하여 프레임의 내용을 어떻게 취급할것인가를 결정하는 여러 포구장치이다. 이것이 무엇을 의미하는가를 리해하기 위하여서는 먼저 통신규약이란 무엇이며 그것이 어떻게 동작하는가를 보아야 한다.

지금까지는 망장치들에 배당된 MAC주소를 리용하여 잘 통신하고 있었다. 체계는 이 번호를 리용하여 다른 체계들과 접촉하고 요구되는대로 정보를 전송하였다.

이와 관련한 문제는 그것이 잘 확장되지 않는것이다. 실지로 만일 서로 통신하려는 2000개의 체계를 가지고 있다면 어떻게 되겠는가? 이것은 하나의 이써네트망에서 대역너비를 가지고 서로 다투는 2000개의 체계를 가지고 있는것으로 된다. 교환기를 사용한다고 하여도 방송프레임들이 많아서 망성능은 크게 떨어 지게 되며 더 많은 체계들을 추가할수 없게 된다. 이런 문제로 하여 IP와 IPX와 같은 통신규약들이 나타나게 되였다.

망통신규약

가장 낮은 수준에서 망통신규약은 망체계가 지리적범위와 공통적인 배선에 의하여 집단 지어 진다는 의미를 제공하는 통신규칙들의 모임이다. 그것이 특정한 집단의 부분이라는것을 지적하기 위하여 이 매개 체계에는 동일한 규약망주소가 배당된다.

망주소는 우편번호와 류사한 종류이다. 어떤 사람이 편지를 부치는데 겉봉투에 《Fritz & Wren, 7 Spring Road》라고 썼다고 하자. 이것이 매우 작은 도시에서 있은 일이라면 그 편지는 아마 쉽게 전달될것이다(LAN에서 MAC주소를 리용한것처럼).

그러나 만일 그 편지가 큰 도시에서 부친것이라면 우편국에서는 그것을 어디로 보낼것인지 모를것이다(우편국직원들은 아마 좋은 웃음거리를 얻었을것이다.).

우편번호가 없으면 그들은 배달을 시도할수도 없다. 우편번호는 이 편지가 배달되여야 할 대체적인 지역을 지정하는 방법을 제공한다. 그 편지를 취급하는 우편국직원은 Spring Road가 어디에 위치하고 있는지를 알 필요가 없다. 그는 그저 우편번호를 보고 그 번호에 책임 있는 우편국에로 그 편지를 전송한다. Spring Road의 위치를 알고 이 지식을 리용하여 그 편지를 배달하는것은 말단우편국이 하는 일이다.

통신규약망주소는 이와 류사하게 동작한다. 규약을 리해하는 장치는 목적지장치의 망주소를 프레임의 자료마당에 첨가한다. 또한 원격체계가 응답을 보내야 하는 경우에 자기의 망주소도 기록한다.

이것이 경로기가 나타나게 되는 리유이다. 경로기는 모든 알려 진 망들에 대한 표를 가지고 있는 규약을 리해하는 장치이다. 그것은 이 표를 리용하여 정보를 그것의 최종목적지까지 보내도록 한다. 경로조종되는 망이 어떻게 동작하는가를 알기 위하여 한가지 실례를 보기로 하자.

경로조종되는 망의 실례

그림 4-13에서 보여 준 망을 가지고 있는데 체계 B가 체계 F에 정보를 전송하려고 한다고 가정하자.

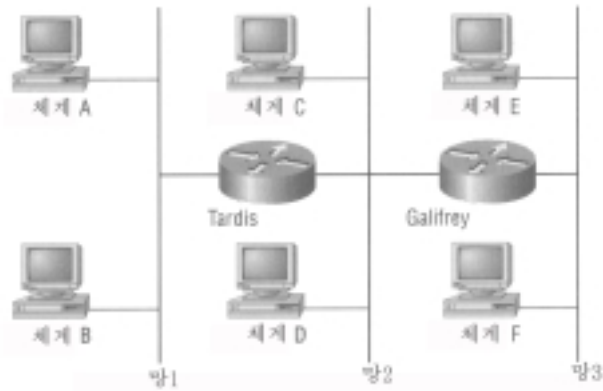



그림 4-13. 경로조종망의 실례

체계 B는 자기의 망주소를 체계 F의것과 비교하는것부터 시작할것이다. 망주소가 같으면 체계 B는 그 체계와 같은 국부망에 있다고 가정하고 정보를 직접 배달하려고 시도한다. 만일 망주소가 다르다면 체계 B는 자기의 경로조종표를 참고한다. 그것이 망 3에 대한 항목을 가지고 있지 않다면 그것은 자기의 기정경로기에로 돌아 가는데 그것은 이 경우에 Tardis이다. 정보를 Tardis에게 전달하기 위하여 체계 B는 Tardis의 MAC주소를 위하여 ARP를 낸다.

다음에 체계 B는 그 자료에 체계 F에 대한 망규약전달정보를 추가하여 Tardis의 MAC주소를 목적지로 리용하는 하나의 프레임을 만든다. 이것은 체계 B가 Tardis가 목적지망에로의 정보전달을 책임지고 있다고 가정하기때문이다.

Tardis가 그 프레임을 받으면 그것은 CRC검사를 진행하여 자료의 무결성을 확인한다. 프레임이 검사되면 Tardis는 머리부와 꼬리부를 완전히 떼낸다. 다음에 Tardis는 그 프레임에 들어 있는 목적지망주소(이 경우에 망 3)를 분석하여 그것이 이 망에 국부적으로 련결되였는가를 알아 낸다. Tardis가 망 3에 직접 련결되지 않았으므로 그것은 자기의 경로조종표를 참고하여 거기로 가는 가장 좋은 경로를 찾아 낸다. 다음에 Tardis는 Galifrey가 망 3에 도달할수 있다는것을 발견한다.

Tardis는 이제 Galifrey가 리용하는 국부MAC주소를 알기 위하여 ARP를 보낸다. 그리고 원천마당에 자기의 MAC주소, 목적지마당에 Galifrey의 MAC주소를 가지는 머리부를 만들어 그 자료파케트의 새로운 프레임을 만들어 낸다. 마지막으로 새로운 CRC값을 꼬리부에 덧붙인다.

이러한 머리부를 뜯어 내고 프레임을 다시 만드는 작업은 매우 큰 작업량인것 같지만 이러한 형식의 통신에서 꼭 필요한 부분이다. 경로기들은 망토막의 경계에 배치된다는것을 상기하라. CRC검사는 나쁜 프레임이 그 망을 통하여 전파되지 않는다는것을 담보하기 위하여 진행한다. 머리부정보는 그것이 망 1에서만 쓸수 있기때문에 떼낸다. Tardis가 그 프레임을 망 2우로 전송하려고 할 때 원래의 원천 또는 목적지MAC주소들은 의미를 가지지 않는다. 그러므로 Tardis는 이 값들을 망 2에서 쓸수 있는것들로 바꾸어야 한다.

머리부의 대부분(14byte중 12byte)이 교체되여야 하므로 그 머리부를 완전히 떼내고 기억기로부터 그것을 다시 만드는것이 더 쉽다. 꼬리부를 떼는것과 관련하여서는 원천

및 목적지MAC주소가 일단 변화되였으므로 원래의 CRC값은 더는 의미가 없게 된다. 그러므로 경로기는 그것을 떼내고 새것을 만들어야 한다.

주 의

규약정보를 포함하는 자료마당을 파케트라고 부른다. 이 용어는 때로 프레임과 같은 의미로 쓰이기도 하지만 파케트는 사실상 프레임의 한 부분만을 서술한다.

Tardis는 그 파케트를 둘러 싸고 하나의 새로운 프레임을 만들었고 그것을 전송할 준비가 되였다. Tardis는 이제 그 프레임을 망 2로 전송하고 그것은 Galifrey에게 수신될 것이다. Galifrey는 그 프레임을 받고 Tardis와 류사한 방법으로 그것을 처리한다. 그는 CRC를 검사하며 머리부와 꼬리부를 떼여 낸다.

그러나 이 점에서 Galifrey는 그것들이 둘다 망 3에 련결되여 있으므로 자기가 체계 F와 규약적련결을 가지고 있다는것을 알게 된다. Galifrey는 그 파케트둘레에서 하나의 새로운 프레임을 만들고 표를 참고하지 않고 그 프레임을 직접 배달한다.

통신규약의 전문성

경로기가 이러한 형식의 기능을 제공하기 위하여서는 리용되고 있는 규약에 대한 규칙들을 알아야 한다. 이것은 경로기가 특정의 통신규약과 련관되여야 한다는것을 의미한다.

어떤 정당한 위상구조적자료흐름을 취급하는 망다리와는 달리 경로기는 위상구조와 리용되는 통신규약을 둘 다 지원할수 있도록 설계되여야 한다. 실례로 망이 Banyan Vines체계를 포함한다면 경로기가 Vines IP를 지원하도록 담보하여야 한다.

경로기는 망에서의 통신량의 흐름을 조종할수 있는 강력한 도구로 될수 있다. 만일 IPX와 IP를 쓰는 망토막을 가지고 있는데 IP만이 회사의 중추망에서 리용하도록 승인되여 있다면 경로기에 IP만을 지원하게 해주면 된다. 그러면 그 경로기는 수신하는 모든 IPX자료흐름을 무시할것이다.

경로기의 중요한 특징은 방송을 막는 능력이다(3장에서 언급한바와 같이 방송은 목적지MAC주소로서 모두 F를 포함하는 프레임들이다.). 경로기의 다른쪽의 임의의 점은 새로운 망이므로 이 프레임들을 막을수 있다.

주 의

망주소와 MAC주소마당에 다 F들을 포함하는 이른바 집단내방송이라고 하는 우의것과 대응되는것이 있다. 이 프레임들은 망주소가 알려 져 있을 때 국부망에 방송하는데 리용된다. 대부분의 경로기들은 기정에 의하여 이 집단내방송들도 차단한다.

대부분의 경로기들은 또한 일정한 자료흐름을 려과하는 능력을 가진다. 실례로 한 회사가 다른 한 회사와 협력한다고 하자. 이때 그 회사는 새로운 망에서의 봉사에 접근하여야 하지만 동업자들이 자기의 봉사기에 접근하는것은 원하지 않는다. 이것을 실행하기 위하여서는 두 망사이에 경로기를 설치하고 다른 회사의 망으로부터 오는 모든 통신대화를 려과하도록 구성한다.

대부분의 경로기들은 자료흐름을 조종하기 위하여 정적파케트려과를 리용한다. 이것이 어떻게 움직이는가 하는것은 제6장에서 구체적으로 취급한다. 지금은 경로기가 보통

의 방화벽에서와 같은 자료흐름조종수준은 제공하지 못한다는것을 알아야 한다. 만일 보안요구가 최소라면 파케트려과는 좋은 선택일수 있다. 어쨌든 자기의 망들을 련결하는데 경로기를 리용하게 될것이다.

망다리/교환기/경로기의 대비고찰

표 4-1은 앞의 절에서 고찰한 정보들을 개괄한것이다. 여기서는 자료련결층에서의 통신량조종(망다리와 교환기)과 망층에서의 통신량조종(경로기)사이의 차이를 인차 알수 있다.

표 4-1 망다리/교환기와 경로기의 비교

망다리(교환기)	경로기
모든 포구들이 같은 망주소리용	모든 포구가 다른 망주소리용
MAC주소에 기초하여 표작성	망주소에 기초한 표작성
MAC주소에 기초한 자료흐름려과	망 또는 호스트정보에 기초한 자료흐름려과
방송프레임을 통과	방송프레임을 차단
모르는 주소에로 전송	모르는 주소에로의 차단
프레임 변경 없음	새로운 머리부와 꼬리부만들기
머리부에 기초하여 전송가능	전송전에 항상 대기

계층-3교환

교환기와 경로기사이의 차이에 대한 명백한 리해를 가진데 기초하여 표면상으로 이 두가지를 서로 맞물리게 하는것으로 보이는 한가지 기술을 고찰하자. 이러한 장치를 설명하는데 계층-3교환, 교환기경로조종 그리고 경로기교환 등 3가지가 같은 내용으로 쓰이고 있다.

그러면 정확히 교환기경로기란 무엇인가? 이 장치는 아주 갱신된 장치는 아니다. 사실상 이 장치는 현재의 경로기기술이 좀 더 진화한것이다. 단어 《교환기》가 덧붙음으로써 이 장치가 제공할수 있는 처리능력의 증가를 강조하고 있다.

이 장치는 보통 표준경로기와 같은 기능을 수행한다. 하나의 자료프레임이 수신되면 기억에 보관되고 CRC검사가 진행된다. 다음에 위상구조적프레임을 자료파케트에서 떼낸다. 보통의 경로기와 꼭같이 교환기경로기는 자기의 경로조종표를 참고하여 가장 좋은 전달경로를 결정하고 자료파케트를 프레임으로 재포장하며 그것을 자기의 길로 전송한다.

그러면 교환기경로기는 표준의 경로기와 어떻게 다른가? 그 대답은 이 장치의 덮개에 있다. 그것의 처리는 전용집적회로(ASIC)장치에 의하여 제공된다. 표준의 경로기에서 모든 처리는 하나의 RISC(축소명령콤퓨터)처리기에 의하여 수행된다. 교환기경로기

에서 요소들은 그 경로조종과정에서의 특정의 과제를 수행하도록 전용화된다. 그 결과로 처리량이 크게 증대된다.

이 장치의 실제적인 목적은 표준경로기보다 더 빨리 정보를 통과시키는데 있다. 이것을 달성하기 위하여 제작자는 처리량을 증대시키는데서 보통의 경로기실현과는 좀 다르게 할것을 선택할수 있다. 실례로 어떤 실현에서는 그 프레임에 대한 CRC검사를 하기 위하여 들어 오는 자료흐름을 완충기억기에 보관하지 않을수 있다. 일단 경로결정을 위한 프레임정보를 알았다면 장치는 즉시 정보를 다른쪽으로 전송하기 시작한다.

보안의 견지에서 보면 이것은 항상 좋은것은 아니다. 확실히 성능은 좋아지지만 차단되여야 할 자료흐름이 우연히 통과하는 일이 있을수 있다. 교환기경로기의 실제적인 목적은 성능이므로 무엇을 통과시키는가에 대하여서는 보통의 경로기처럼 구체적으로 따지지 않을수 있다.

계층-3교환은 계속 발전하여 이제는 오래동안 잘 사용하여 온 경로기를 교체할수 있는것으로 간주되게 되였다. 대부분의 현대적인 경로기들은 초당 100만파케트이상을 처리할수 있도록 발전하였다. 보통 매우 높은 통신량은 주로 중추망에서만 요구된다. 현재까지 이것으로 하여 교환기는 망의 이 분야에서 우위를 차지하였었다.

그러나 교환기경로조종은 보통의 교환기의 교체물로서 보안의 견지에서 리로울수 있다. 자료흐름을 충돌령역이 아니라 실제적인 부분망에 격리하는 능력으로 하여 망의 이 분야에서 전체적인 새로운 조종수준을 가능하게 하고있다.

경로기와 류사하게 어떤 교환기경로기들은 접근조종목록을 지원하는데 이것은 망관리자로 하여금 어느 체계가 매개 부분망들사이에서 통신할수 있으며 그것들이 어떤 봉사를 접근할수 있는가를 처리할수 있게 한다. 이것은 이전의 교환기가 제공하는것보다 매우 높은 수준의 조종이다. 교환기경로조종은 성능을 떨굼이 없이 내부망의 보안을 강화하는데 도움이 될수 있다. 만일 보안요구가 그리 높지 않다면 교환기경로기는 바로 보안방책을 증강하는것으로 될수 있다.

주 의

제6장의 Cisco경로기에서 접근조종목록(ACL)을 실현하는 몇가지 실례를 보게 될것이다.

요 약

이 장에서는 많은 기초적문제들을 취급하였다. 보안의 관점에서 통신의 특성들을 고찰하였으며 전송매체와 장치들을 살펴 보았다. 또한 대표적인 망장치들에 의하여 어떤 자료흐름조종선택들이 준비되여 있는가를 고찰하였다.

다음의 몇개 장들에서는 보안방책들을 실현하기 위하여 설계된 체계들을 고찰할것이다. 방화벽으로부터 시작하여 침입검출체계를 고찰하게 된다.

제5장. 방 화 벽

이 장에서는 방화벽과 그 실현에 대하여 고찰한다. 모든 방화벽이 다 같은 방법으로 동작하는것이 아니므로 그것이 제공하는 보안에 기초하여 방화벽을 선택하며 그것이 기업의 요구에 잘 맞는가를 확인하도록 한다. 실례로 어떤 회사가 방화벽이 AOL의 Instant Messenger를 지원하지 않으며 IM이 결정적인 기업기능이라면 그저 도선절단기나 하나 사는것이 더 좋을수도 있다. 방화벽을 고찰하기전에 그것을 구입할것인가를 결정하기 위하여 어떤 정보를 수집하여야 할것인가를 보기로 한다.

접근조종방책의 정의

구입하려는 방화벽의 형태 또는 상표를 선택하기에 앞서 당신은 매우 간단한 한가지 문제를 알아야 한다(이것을 대답하기에는 시간이 많이 걸릴수도 있다.).

망으로 드나드는 자료통신량흐름을 취급하는 규칙들이란 어떤것들인가? 이 문제에 대한 대답은 망의 접근조종방책을 형성할것이다. 접근조종방책이란 망에서 어떤 형식의 접근이 허용되는가를 서술한 하나의 기업방책이다. 실례로 기관은 다음과 같은 방책을 가지고 있을수 있다. 《우리의 내부사용자들은 인터네트Web싸이트와 FTP싸이트에 접근할수 있으며 SMTP우편을 보낼수 있다. 그러나 우리는 인터네트로부터 우리 내부망에로 들어 오는 SMTP우편만을 허용할것이다.》

접근조종방책은 내부망의 각이한 구역들에 적용할수 있다. 실례로 한 기관은 자기의 기업상대를 지원하기 위하여 WAN련결을 가지고 있을수 있다. 이 경우에 이 련결에 의한 접근범위를 제한하여 정의함으로써 그것이 원래의 목적만으로만 리용되도록 담보하려고 할것이다.

접근조종방책은 망의 여러 부분에로 드나드는 자료흐름의 방향을 정의한다. 또한 어떤 형식의 자료흐름이 접수가능하고 어떤것이 차단되는가 하는것도 규정한다. 접근조종방책을 정의할 때 많은 각이한 파라메터들을 리용하여 자료흐름을 서술할수 있다. 방화벽을 가지고 실현할수 있는 몇가지 공통적인 서술자들을 표 5-1에 주었다.

일러두기

만일 기관이 접근조종방책을 가지고 있지 않다면 그것을 만들어야 한다. 명백히 정의된 접근조종방책은 정확한 방화벽제품들을 선택하는것을 담보한다. 1만딸라나 들여서 새 방화벽프로그람을 사는것보다 나쁜 일은 없지만 게다가 그 프로그람이 기관이 원하던것들을 다 하지 못한다면 더욱더 유감스러운 일로 될것이다.

앞으로 어떤 형식의 접근조종을 요구할것인가를 상상하고 창조하여야 한다. 이렇게 하는것은 자기의 방화벽문제를 인차 해결하지 않도록 담보한다. 어떤 기관들에서는 인터네트로부터의 자기들의 국부망에로의 접근에 대하여 관심을 돌리지 않고 있다. 그러

표 5-1 접근조종서술자들

ˏ 술	정 의
방향 (Direction)	방향에 따르는 허용가능한 자료흐름의 서술. 실례로 인터네트로부터 내부망에로의 자료흐름(내부로) 또는 내부망으로부터 인터네트에로의 자료흐름(밖으로)
봉사	접근되는 봉사기응용프로그람의 형태. 실례로 Web접근(HTTP), 파일전송규약(FTP), 단순우편전송규약(SMTP)
특정호스트	때로 방향만을 규정하는것이 부족할 때가 있다. 실례로 들어 오는 HTTP접근은 허용하지만 하나의 특정콤퓨터에게만은 허용하지 않을수 있다. 반대로 하나의 콤퓨터에만 인터네트Web봉사기접근을 허용할수 있다.
개별사용자	많은 기관들은 일정한 개인이 특정의 활동을 하도록 하지만 다른 사람에게는 이러한 형태의 접근을 원하지 않을수 있다. 실례로 회사 CEO는 인터네트로부터 내부자원에 접근하는것을 허용되고 있다. 이 경우에 그 접근조종방책을 집행하는 장치는 접근을 얻으려 하는 사람을 인증하여 CEO만이 통과되도록 담보한다.
시간	때로 일정한 시간동안 접근을 제한하려고 할수 있다. 실례로 한가지 접근조종방책에서는 《내부사용자는 인터네트Web봉사기를 5시부터 7시사이에만 접근할수 있다.》라고 규정하고 있다.
공개 또는 비밀	때로 공공망을 리용하여(프레임중계 또는 인터네트와 같은) 비밀자료를 전송하는것이 유리할 때도 있다. 접근조종방책은 정보가 두 특정호스트 또는 전체 망토막을 통과할 때 암호화되여야 한다는것을 정의할수 있다.
봉사의 질	기관은 준비된 대역너비에 기초하여 접근을 제한하려고 할수 있다. 실례로 인터네트로부터 접근될수 있는 하나의 Web봉사기를 가지고 있으면서 이 체계에로의 접근은 항상 응답되여야 한다는것을 담보하려고 할수 있다. 잠재적인 의뢰기가 현재 Web봉사기를 접근하고 있을 때 내부사용자는 제한된 대역너비준위에서 인터네트에 접근하여야 한다는 접근조종방책을 세울수 있다. 의뢰기가 그 봉사기에 접근하고 있을 때 내부사용자들은 인터네트자원을 접근하기 위하여 준비되여 있는 대역너비를 100% 다 가질수 있다.
역할	개별사용자에게 접근을 제한하는것과 류사하게 관리자는 류사한 접근요구를 가지는 개인들을 집단으로 만들기 위한 역할을 리용한다. 이 집단화는 접근조종의 복잡성을 간단하게 하며 관리부담을 쉽게 한다.

나 앞으로는 외부의 의뢰자들이 인터네트에 기초한 원격접근을 요구하리라는것을 타산하여야 한다. 항상 현재의 요구만에 기초하여서가 아니라 균형이 맞게 생각하는것이 중요하다.

방화벽의 정의

방화벽이란 망자료흐름이 접근점들을 통과할 때 그것에 대하여 접근조종방책을 집행하는 체계 또는 체계들의 집단이다. 일단 제공하려는 련결의 수준을 결정하였다면 이 범위를 초과하는 추가적인 접근을 허용하지 않도록 담보하는것이 방화벽의 과제이다. 망의 모든 사용자들이 접근조종방책을 지키도록 담보하는것은 방화벽에 달려 있다.

방화벽은 그것의 목적이 자료흐름을 조종하는것이라는 점에서는 다른 망장치들과 류사하다. 그러나 다른 망장치들과 달리 방화벽은 그 자료파케트가 무엇인가를 고려하여 자료흐름을 조종하여야 한다.

실례로 망다리는 자료흐름을 목적지 MAC주소에 기초하여 려과한다. 만일 호스트가 부정확하게 목적지 MAC주소를 붙이고 또 망다리가 주의를 돌리지 않고 그 파케트를 틀린 목적지로 보낸다고 하여도 그 망다리는 고장났다거나 부정확하다고 보지 않는다. 호스트가 망규칙을 지켜야 하는것이고 그것이 이 규칙을 어겼다면 호스트가 잘못이지 망다리가 아닌것이다.

그러나 방화벽은 호스트들이 그것을 통과하는 정보를 훔치기 위하여 그를 속이려 할수 있다고 가정하여야 한다. 방화벽은 통신규칙들을 지팽이로 리용할수 없으며 오히려 그 통신규칙들이 지켜 지지 않고 있다고 가정하여야 한다. 이것은 방화벽설계에 큰 부하를 가하고 있으며 매개 우발적요소들까지도 다 계획하도록 할것을 요구하고 있다.

언제 방화벽이 요구되는가

보통 내부망과 인터네트사이에서 접근조종은 진행되지만 방화벽이 요구될수 있는 정황은 매우 많다.

전화가입모뎀풀(Dial-in Modem pool)

방화벽은 전화가입모뎀풀로부터의 접근을 조종하는데 리용될수 있다. 실례로 전화가입사용자들이 하나의 우편체계만을 접근할수 있도록 규정하는 접근조종방책을 가지고 있을수 있다. 회사나 기관들은 다른 내부봉사기 또는 인터네트에 접근하는것을 허용하려고 하지 않는다. 방화벽은 이러한 방책을 실현하는데 리용될수 있다.

기업상대와의 외부적련결

많은 기관들은 기업상대와 영구적인 원격련결을 가지고 있다. 이것은 어려운 정황을 만들수 있다. 련결은 기업을 위하여 요구되는것이나 어떤 사람은 보안이 기관에 의하여 관리되지 않는 구역으로부터 내부망에 접근할수 있다. 방화벽은 이 련결들로부터의 접근

을 조절하고 문서화하는데 리용될수 있다.

부서들사이에서

어떤 회사들(무역회사와 같은)은 서로 다른 망지역사이에서 내부방화벽을 가지고 있어야 한다. 이것은 내부사용자만이 요구하는 정보에 접근하도록 담보하기 위한것이다. 이 두 망들사이의 련결점에서 방화벽은 접근조종을 집행한다.

방화벽의 류형

모든 방화벽이 같이 만들어 진것은 아니다. 망주변에서의 접근을 조종하기 위하여 여러가지 기술들이 리용되였다. 가장 널리 쓰이는것은 다음과 같은것들이다.

- 정적파케트려과
- 동적파케트려과
- 상태려과
- 대리자

정적파케트려과

정적파케트려과는 파케트머리부에 보관된 정보를 리용하여 자료흐름을 조종한다. 파케트가 려과장치에서 수신될 때 파케트머리부안에 보관된 자료의 속성들이 접근조종방책과 비교된다(접근조종목록 또는 ACL이라고 부른다.). 이 머리부정보가 ACL과 어떻게 비교되는가에 따라 그 자료흐름은 허용되든가 차단된다.

정적파케트려과기는 자료흐름을 조절할 때 다음의 정보를 리용한다.

- 목적지 IP주소 또는 부분망
- 원천 IP주소 또는 부분망
- 목적지봉사포구
- 기발(TCP에서만)

TCP기발마당

전송층에서 TCP가 리용될 때 정적파케트려과는 자료흐름조종결정을 만들기 위하여 TCP머리부의 기발마당을 리용할수 있다. 그림 5-1은 TCP/IP파케트의 파케트해신을 보여 준다. 조종비트마당은 어느 기발이 설정되였는가를 보여 준다. 기발들은 설정되거나(2진값 1) 또는 재설정(2진값 0)된다.

그러면 기발마당은 무엇을 표시하는가? 제3장에서 고찰한 TCP3-파케트련결신호로부터 서로 다른 기발값들은 통신대화의 여러가지 상태를 식별하는데 리용된다는것을 알수 있다. 이 기발마당은 수신측 호스트에게 그 파케트가 나르고 있는 자료에 대한 몇가지

보충적인 정보를 준다.

그림 5-1. TCP/IP 파케트해신

표 5-2는 기발들과 그것들의 리용을 목록으로 보여 준다.

기발마당은 정적파케트려과에서 중요한 역할을 논다. 그것은 방화벽이 어떤 특정의 포구에서 나오거나 또는 특정의 호스트에로 가는 모든 자료흐름들을 막는것은 아니기때문이다.

실례로 다음과 같은 접근조종방책을 가지고 있을수 있다. 《우리의 내부사용자들은 인터네트우의 임의의 봉사로 접근할수 있으나 내부망에로 향하는 모든 인터네트자료흐름은 막아야 한다.》 이것은 ACL이 인터네트로부터 오는 모든 자료흐름들을 막아야 한다는것처럼 들리지만 사실상 그렇지 않다.

모든 통신은 두 단계과정을 표현한다. 어떤 사람이 Web싸이트를 접근할 때 그는 하나의 자료요청을 만들며(단계 1) Web싸이트는 요청한 자료를 돌려 보냄으로써 그에게 응답한다(단계 2). 이것은 단계 2동안에 인터네트호스트로부터 내부체계에로 자료가 오기를 기다리고 있다는것을 의미한다. 접근조종방책의 뒤부분을 그대로 받아 들인다면(《…내부망으로 향하는 모든 인터네트자료흐름은 막아야 한다.》) 우리의 응답들은 결코 요청한 호스트에 돌아 오지 못할것이다. 우리는 《효과적인 보안장치로서의 도선절단기》에로 돌아 온것이나 같다. 우리의 방화벽은 하나의 완전한 통신대화를 허용하지 않는다.

이로부터 기발마당이 리용된다. TCP3-파케트련결신호동안에 시작하는 체계는 SYN=1이고 다른 모든 기발들은 0인 파케트를 전송한다는것을 상기하시오. 이것은 한 체계가 다른 체계에 련결을 설정할 때 하는것이다. 파케트려파기는 TCP대화들을 조종하기 위하여 이 일의적인 기발설정을 리용한다. 초기련결요청을 막으면 두 체계사이의 자료대화는 설정될수 없다.

그러므로 접근조종방책이 기술적으로 보다 정확한것으로 되도록 하기 위해서 다음과

갈이 말해야 한다. 《SYN=1이고 다른 모든 기발들은 0값을 가지는 내부망으로 향하는 모든 인터네트자료흐름들은 막아야 한다.》 이것은 명백히 망주변을 잠그기 위한 가장

표 5-2 TCP/IP 기발

TCP 기발	기발의 내용
ACK(Acknowledgement)	이 자료가 한 자료요청에 대한 응답이라는것과 답례번호마당에 유용한 정보가 있다는것을 지시한다.
FIN(Final)	송신체계가 현재의 대화를 끝내려고 한다는것을 지적한다. 보통 통신대화의 매 체계는 련결을 실제적으로 닫기전에 하나의 FIN을 내보낸다.
PSH(Push)	전송체계가 전송하기전에 자료들을 대기하지 못하도록 한다. 많은 경우에 전송체계가 전송하기전에 적은 자료량을 대기하게 하여 보다 적은 파케트가 만들어 지게 하는것이 보다 효과적이다. 수신측에서 Push는 원격체계가 그 자료를 대기하지 못하게 하지만 웃층규약준위에로 가는 정보는 즉시 밀어 낸다.
RST(Reset)	현재 통신대화의 상태를 재설정한다. Reset는 회복불가능한 전송오유가 발생할 때 리용된다. 이것은 전송층이 다음과 같이 말하는것에 해당된다. 《당신은 내 말을 듣고 있었는가? 내가 그것을 다시 말해야 하는가?》 이것은 대체로 응답 없는 호스트에 의하여 발생한다.
SYN(Synchronize)	통신대화를 초기화하는데 리용된다. 이 기발은 통신과정의 어떤 다른 부분들에서는 설정되지 말아야 한다.
URG(Urgent)	전송체계가 높은 우선권을 가지는 정보를 가지고 있다는것, 긴급지시기마당안에 유용한 정보가 있다는것을 지적한다. 한 체계가 URG기발이 설정된 파케트를 수신한다면 다른 자료보다 먼저 그 정보를 처리한다. 이것을 대역외자료처리라고 말한다.

안전한 방법은 아니다. 기발값들을 리용하여 공격자는 정적파케트려파기를 속이고 나쁜 자료흐름을 통과시키게 할수 있다. 이 방법으로 이 도적들은 이 보안장치들을 한걸음 앞지를수 있다.

FIN스캐너

간단한 파케트려파기는 포구주사를 막을수 있으므로 어떤 사람들은 뭔가 해보기로 결심하였다. 간단한 포구스캐너는 결국 FIN스캐너로 진화되였다. FIN스캐너는 포구스캐너와 류사한 원리로 동작하는데 전송되는 파케트는 FIN=1, ACK=1이고 다른 모든 기발들은 0이다.

우리의 파케트려파기는 SYN=1이고 다른 모든 기발들은 0인 파케트들만 막으려 하므로 이 파케트들은 쉽게 통과된다. 그 결과는 공격자가 돌아 오는 자료흐름을 분석하여 어느 호스트가 어떤 봉사를 제공하고 있는가를 결정할수 있게 한다는것이다. 만일 목적지호스트가 ACK=1, RST=1(존재하지 않는 봉사에 대한 일반적인 체계응답)로 되돌려 보낸다면 그 쏘프트웨어는 이것이 리용되지 않는 포구라는것을 알게 된다. 그러나 만일 목적지호스트가 ACK=1, FIN=1(련결을 닫는데 동의)을 돌려 보낸다면 FIN스캐너는 그 포구를 감시하는 봉사가 있다는것을 안다. 이것은 우리의 파케트려파가 이러한 주사식검사를 막는데 쓸수 없다는것을 의미한다.

실례로 포구스캐너라고 하는 쏘프트웨어프로그람이 있는데 그것은 목적지호스트를 검사하여 어떤 봉사포구들이 열려 있는가를 알아 볼수 있다. 포구스캐너는 지정된 구역안의 모든 봉사포구들에 련결요청(SYN=1)을 보낸다. 이 련결요청들중 일부가 목적지호스트가 련결요청답례(SYN=1, ACK=1)를 보내게 할수 있으면 이 쏘프트웨어는 그 포구를 감시하는 봉사가 있다는것을 알게 된다.

UDP 자료흐름의 파케트려과

TCP자료흐름은 조종하기가 그리 어렵지 않으나 UDP자료흐름은 좀 어렵다. 이것은 UDP가 련결의 상태에 대하여 TCP보다 적은 정보를 제공하기때문이다. 그림 5-2는 UDP머리부의 파케트해신을 보여 준다.

우리의 UDP머리부는 대화의 상태를 지적하기 위한 기발들을 리용하지 않는다는것에 주목하여야 한다. 이것은 파케트가 자료요청인지 또는 이전의 요청에 대한 응답인지 결정하는 방법이 없다는것을 의미한다. 즉 자료흐름을 결정하는 방법이 없다는것을 의미한다. 자료흐름을 조절하는데 리용될수 있는 유일한 정보는 원천 및 목적지포구번호이다. 그런데 어떤 봉사들은 같은 원천 및 목적지포구번호를 리용하므로 이 정보는 많은 정황에서 적게 리용된다.

실례로 두 령역이름봉사기(DNS)가 정보를 교환하고 있을 때 그것들은 원천 및 목적지포구번호로 53을 리용한다. 많은 다른 봉사들과 달리 그것들은 1023보다 큰 응답포구를 리용하지 않는다. 이것은 정적파케트려파기가 DNS자료흐름을 한 방향으로만 제한하는 효과적인 방법이 없다는것을 의미한다. 그러므로 포구 53에로의 들어 오는 자료흐름을 막을수 없다. 왜냐하면 그것은 자료응답과 함께 자료요청도 막기때문이다.

그림 5-2. UDP머리부해신

이것으로 하여 많은 경우들에서 정적파케트려과기에 의하여 UDP자료흐름을 조절하는 유일하게 효과적인 방법은 그 포구를 막든지 또는 그것을 통과시키게 하고 좋은 결과가 있기를 바라는것뿐이다. 대부분의 사람들은 UDP자료흐름을 꼭 통과시켜야 할 필요가 없다면 대체로 전자의 경우로 고정시키고 있다.

ICMP의 파케트려과

인터네트조종통보문규약(ICMP)은 IP규약에 대한 배경지원을 제공한다. 그것은 사용자자료를 나르는데 리용되지 않고 모든것이 원만하게 돌아 가고 있다는것을 보증하기 위한 관리과제를 위하여 리용된다. 실례로 Ping은 ICMP를 리용하여 두 호스트사이에 련결이 있다는것을 보증한다. 그림 5-3은 ICMP머리부의 파케트해신을 보여 준다.

주 의

ICMP는 봉사포구를 리용하지 않는다. ICMP파케트의 형식을 식별하기 위한 형식(Type)마당과 현재의 대화에 대한 보다 상세한 정보를 제공하기 위한 코드(Code)마당이 있다.

코드마당은 좀 혼돈이 될수 있다. 실례로 그림 5-3에서 코드는 Protocol Unreachable :Host Unreachable로 되여 있다. 이것은 목적지체계가 응답하지 않고 있다고 생각하게 할수 있다. 만일 ICMP파케트에 대한 원천 IP주소를 Original IP Packet Header의 뒤에 있는 목적지주소와 비교한다면 그것들이 같다(10.1.1.100)는것을 알게 될것이다. 그러므로 목적지가 사실상 《도달불가능》하다면 어떻게 그것이 이 응답을 보낼수 있었을가?

이 두 코드들의 결합은 사실상 요청된 봉사가 준비되여 있지 않았다는것을 의미한다. 만일 그림 5-3의 웃부분을 보면 이 응답을 촉발시킨 전송은 resume.txt에 대한 TFTP요청이 있다는것을 알수 있다. 목적지호스트만이 규약도달불가능오유를 낼수 있다. 표 5-3은 ICMP파케트에 대한 여러가지 형식마당값들을 식별한다.

그림 5-3. ICMP머리부

주 의

UDP는 기발마당을 리용하지 않는다. 이것으로 하여 UDP는 전송체계가 봉사가 준비되여 있지 않다는것을 알도록 하는데 쓸수 없다. 이 문제를 해결하기 위하여 ICMP가 리용되여 전송체계에 알리게 된다.

표 5-3 ICMP Type 마당의 값들

Type	이 름	설 명
0	Echo Reply	echo요청에 응답
3	Destination unreachable	목적지부분망, 호스트 또는 봉사에 도달할 수 없다.
4	Source Quench	수신체계 또는 그 경로에 따르는 경로기가 고장나서 들어 오는 자료흐름을 통과시키지 못한다. 이것을 수신하는 체계는 자기의 전송속도를 감소시켜야 한다. 이것은 수신체계가 파부하로 하여 자료를 잃어 버리지 않도록 담보하기 위한것이다.
5	Redirect	국부호스트에 그 호스트가 전송하고 있는 자료를 더 잘 전송할수 있는 또 하나의 경로기가 있음을 알린다. 이것은 국부경로기에 의하여 전송된다.
8	Echo	목표체계가 Echo응답을 보낼것을 요청한다. Echo는 점대점련결을 확인하며 응답시간을 측정하는데 리용된다.

표계속

Type	이 름	설 명
9	Router Advertisement	경로기가 부분망에서 자기자신을 식별하기 위하여 사용한다. 이것은 경로정보를 나르지 않으므로 경로조종규약은 아니다. 이것은 그저 부분망우의 호스트가 그것들의 국부경로기의 IP주소를 알도록 하는데 리용된다.
10	Router Selection	호스트가 다음주기갱신을 기다리지 않고 경로기에 질문할수 있게 하는것
11	Time Exceeded	전송체계에 파케트머리부의 TTL값이 초과되고 정보가 도달될수 없음을 알린다.
12	Paramater Problem	ICMP로 식별할수 없는 문제가 발생하였을 때 전송체계에 보내는 다목적응답
13	Timestamp	련결의 속도를 측정하려고 할 때 리용된다. Echo요청과 비슷하나 이 요청에 대한 빠른 응답이 결정적인것이다.
14	Timestamp Reply	Timestamp요청에 대한 응답
15	Information Request	Bootp와 DHCP에 의하여 교체되였다. 이 요청은 원래 IP주소를 발견하기 위하여 자체구성체계들에서 리용되였다.
16	Information Reply	Information Request에 대한 응답
17	Address Mask Request	체계가 동적으로 국부망에 어떤 부분망이 리용될것인가를 묻도록 한다. 만일 응답이 수신되지 않으면 호스트는 자기의 주소클라스에 적당한 부분망마스크를 가정하여야 한다.
18	Address Mask Reply	주소마스크요청에 대한 응답
30	Traceroute	한 IP호스트로부터 다른것에로의 경로를 추적하는 효과적인 수단을 제공한다. 이 선택은 모든 중계경로기들이 이 ICMP형식을 인식하도록 프로그람화되였을 때에만 리용된다. 실현은 Ping명령을 리용하는 교환기설정을 통하여 진행된다.

표 5-4는 ICMP형식이 목적지도달불가능(Type=3)일 때 리용될수 있는 코드들을 보여준다.

표 5-4 ICMP Type3 코드마당값들

코드	이 름	설 명
0	Net Unreachable	경로조종오유(경로정보가 없는것과 같은)나 불충분한 TTL값으로 하여 목적지망에 도달할수 없다.
1	Host Unreachable	경로조종오유나 불충분한 TTL값으로 하여 목적지호스트에 도달할수 없다.
2	Protocol Unreachable	접속한 목적지호스트가 요구되는 봉사를 제공하지 않는다. 이 코드는 대표적으로 호스트로부터 귀환되며 다른것들은 모두 그 경로에 따르는 경로기로부터 귀환된다.
4	Fragmentation Needed and Don't Fragment Was Set	배달하려는 자료가 보다 작은 파케트크기를 가지는 망을 통과하여야 하는데 《don't fragment》비트가 설정되여 있다.
5	Source Route Failed	전송된 파케트에는 그 경로가 목적지호스트뒤에 있어야 한다고 지적되여 있는데 경로정보가 정확치 않다.

표 5-5는 ICMP type가 redirect(Type=5)일 때 리용될수 있는 코드들을 보여 주고 있다.

표 5-5 ICMP Type5 코드마당값들

코드	이 름	설 명
0	Redirect Datagram for the Network(or Subnet)	국부망우의 또 하나의 경로기가 목적지부분망에로의 보다 좋은 경로를 가지고 있다는것을 지시한다.
1	Redirect Datagram for the Host	국부망우의 또 하나의 경로기가 목적지호스트에로의 보다 좋은 경로를 가지고 있다는것을 지적한다.

Type와 Code마당의 값들에 기초하여 려과를 진행하면 간단히 원천 및 목적지IP주소들을 보는것보다 좀더 세밀한 조종을 할수 있다. 그러나 모든 파케트려과기가 다 모든 Type와 Code들을 리용할수 있는것은 아니다. 실례로 많은 려과기들은 Code값은 고려하지 않고 목적지도달불가능인 Type=3을 려과해 낸다. 이러한 제한은 엄중한 통신문제점들을 초래할수 있다.

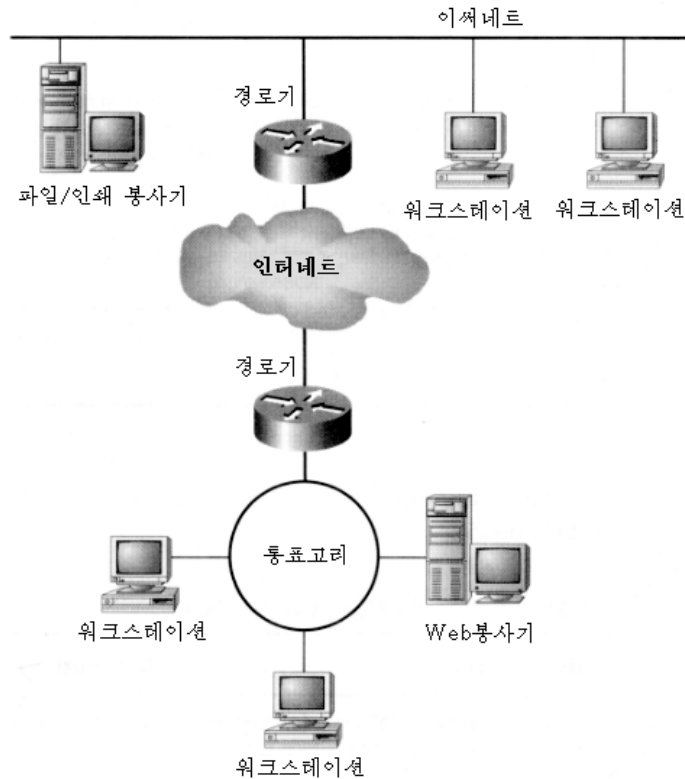



그림 5-4. 목적지도달불가능한 통보문을 막는 문제

이제 그림 5-4에 보여 준것과 류사한 망구성을 가지고 있다고 가정하자. 그 국부망은 통표고리형위상구조를 가지고 있고 원격기업상대는 이써네트망을 가지고 있다. 자기의 기업상대에게 최신의 제품갱신정보와 개발정보를 받기 위하여 국부Web봉사기에 접근하게 하려고 한다.

이제 경로기가 들어 오는 ICMP목적지도달불가능통보문을 막고 있다고 가정하자. 외부공격자가 틀린 호스트도달불가능(Type=5, Code=1)통보문을 보내지 못하게 함으로써 봉사거부공격을 막는 방법으로 하였다. 경로기가 파케트려과능력을 제한하였으므로 모든 ICMP Type=5자료흐름을 막아야 한다.

그러나 이것은 어떤 문제들이 생기게 할수 있다. 기업상대의 종업원들이 그 국부Web봉사기에 접근하려고 할 때 그들은 그 어떤 HTML페지도 볼수 없게 될수 있다. 이 문제는 다음과 같이 나타나며 혼돈될수 있다.

- 이써네트토막에 위치한 워크스테이션의 열람기는 목적지호스트이름을 IP주소로 변환하는것처럼 보인다.
- 그 열람기는 목적지Web봉사기에 련결한것처럼 보인다.
- 만일 어느 한 경로기가 대화가입등록을 제공한다면 자료흐름은 두 체계사이에서 흐르는것으로 나타난다.
- 국부Web봉사기우에서의 가입등록은 그 워크스테이션이 그 Web봉사기에 련결

되고 많은 파일들이 제공되였다는것을 의미한다.

그러면 무엇이 잘못되였는가? 공교롭게도 모든 Type=3인 자료흐름들을 막음으로써 Fragmentation Needed(Type=3, Code=4) 오유통보문도 막았다. 이것은 경로기로 하여금 전송되는 자료흐름의 평균전송단위(MTU)를 조절하지 못하게 한다.

MTU는 하나의 자료파케트에 의하여 전송될수 있는 최대유효자료크기를 의미한다. 이써네트환경에서 MTU는 1.5KB이다. 통표고리형환경에서는 MTU가 16KB만큼 클수 있다. 경로기가 목적지망에 대하여 너무 큰 파케트를 받으면 그것은 전송체계에 요청을 보내여 그 자료를 보다 작은 덩어리로 쪼갤것을 요구한다(ICMP Type=3, Code=4). 경로기가 이 자료를 자체로 토막화하려고 하면 또 자기의 완충기억에 자리가 있는가 하는 문제가 제기된다. 그러므로 원격체계가 보다 작은 파케트를 전송하도록 하는것이 더 쉽다.

그래서 그림 5-4에서의 자료흐름을 본다면 다음과 같다.

1. 하나의 이써네트워크스테이션이 HTML자료요청을 만든다.
2. 이 요청이 목적지Web봉사기에로 전달된다.
3. 두 체계는 64byte파케트를 리용하여 TCP 3-파케트련결신호를 수행한다.
4. 일단 련결신호가 완성되면 Web봉사기는 16KB MTU를 리용하여 자료요청에 응답한다.
5. 이 응답은 원격이써네트망에 있는 경로기에 도착한다.
6. 이써네트경로기는 토막화요청(ICMP Type=3, Code=4)을 Web봉사기에 보내여 1.5KB MTU를 사용할것을 요구한다.
7. 이 요청은 통표고리형망의 경계경로기에로 돌아 간다.
8. 이 경로기는 자기의 ACL을 검사하고 모든 목적지도달불가능통보문(ICMP Type=3)을 중단하도록 하여 그 파케트를 취소한다.

토막화요청은 국부망에로 돌아 오지 않으며 원격기업상대는 목적하였던 Web페지를 볼수 없다. 정적파케트려과를 리용할 때 항상 막거나 허용하고 있는 자료흐름의 결과를 자기가 완전히 리해하도록 하여야 한다.

정적파케트려과에 대한 요약

정적파케트려과기는 비지능적인 려과장치이다. 이것들은 발전된 공격형태들은 거의 막아 내지 못한다. 이것들은 어느 자료흐름이 허용되고 어느 자료흐름은 막아야 하는가를 결정하는데 최소량의 정보만을 리용한다. 많은 경로기들은 정적파케트려과를 수행하는 능력을 가지고 있다.

동적파케트려과

동적파케트려과는 정적파케트려과보다 한걸음 전진한것인데 통신대화의 상태를 감시하기 위한 련결표를 가지고 있다. 그것은 그저 기발설정에만 의존하지 않는다. 이것은 자료흐름을 더잘 조종하는데 리용될수 있는 강력한 기능으로 된다.

실례로 한 공격자가 어떤 체계에 그것을 기능정지시키도록 설계된 내용을 가지는 자료파케트를 보낸다고 하자. 공격자는 이 파케트가 내부체계가 요청한 정보에 대한 응답으로 보이도록 하기 위하여 어떤 속임수를 쓸수 있다. 보통의 파케트려과기는 이 파케트를 분석하여 보고 ACK비트가 설정된것을 알고는 이것이 자료요청에 대한 응답으로 보고 속히우게 된다. 그리고 그것을 내부체계로 운수 좋게(공격자에게는) 통과시킨다.

그러나 동적파케트려과는 그렇게 쉽게 속지 않는다. 정보가 수신되면 동적파케트려과기는 자기의 련결표(때로는 상태표라고도 부른다.)를 참고한다. 표항목들을 조사하여 보고 동적파케트려과기는 내부체계가 이 외부체계와 실제적으로 련결되여 있지 않으며 자료요청을 보내지 않았다는것을 알게 된다. 이 정보는 명백히 요구되지 않았으므로 동적파케트려과기는 그 파케트를 버리게 된다.

동적파케트려과기의 동작

동적파케트려과기가 보안을 얼마나 강화하는가를 더 잘 알기 위하여 그것이 어떻게 동작하는가를 보기로 하자. 그림 5-5에서 두개의 분리된 망구성을 볼수 있다. 하나는 내부호스트가 정적파케트려과에 의하여 보호되는것이고 또 하나는 동적파케트려과를 리용하는것이다.

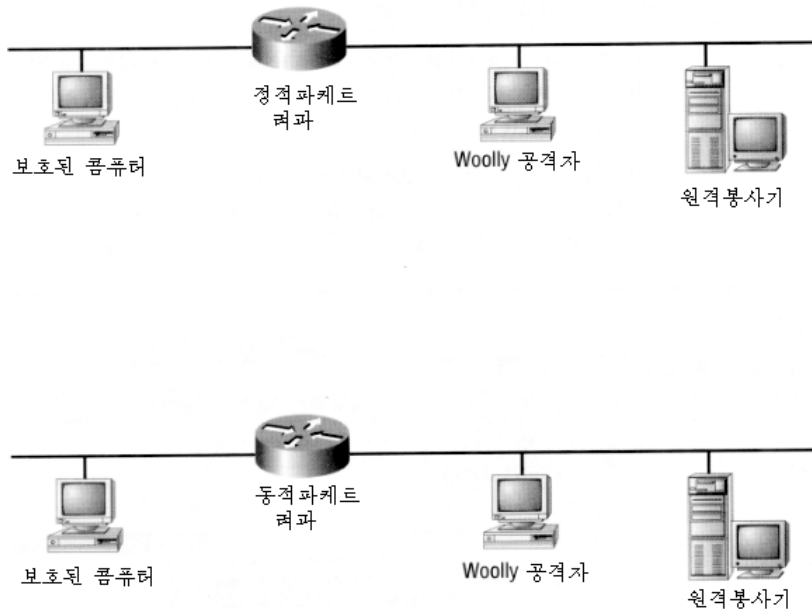



그림 5-5. 정적 및 동적파케트려과사이의 차이

이제 이 두 방화벽장치들이 어떻게 자료흐름조종을 하는가를 알기 위하여 몇가지 접근규칙들을 고찰하자. 두 방화벽에서 다 ACL은 다음과 같이 규정한다.

- 보호된 호스트는 원격봉사기와 임의의 봉사대화를 설정할수 있다.
- 이미 설정된 임의의 대화는 통과를 허용한다.
- 모든 다른 자료흐름은 정지된다.

첫번째 규칙은 보호되는 호스트가 원격봉사기와의 련결을 설정하는것을 허용한다. 이것은 SYN비트가 1인 파케트가 통과되도록 허용되는 유일한 경우는 원천주소가 보호되는 호스트의것이고 목적지는 원격봉사기인 경우라는것을 의미한다. 바로 이때 원격봉사기에서의 임의의 봉사는 접근가능하다.

두번째 규칙은 포괄적인것이다. 기본적으로 그것은 다음과 같이 규정하고 있다. 《자료흐름이 이전에 설정된 련결의 부분으로 나타난다면 그것을 통과시키시오.》 다른 말로 하면 SYN비트가 설정되지 않고 다른 모든 비트들이 0이라면 그 자료흐름은 통과라는것이다.

세번째 규칙은 어떤 자료흐름이 첫 두개의 규칙들중 어느것에 꼭 맞지 않는다면 안전을 위하여 그것을 버리라는것이다. 이 두 방화벽은 다 좋은 ACL을 리용한다. 그 차이는 자료흐름을 조종하기 위하여 매개에 준비되여 있는 정보의 량에 있다. 어떤 자료흐름을 전송하고 무엇이 발생하는가를 보기로 하자.

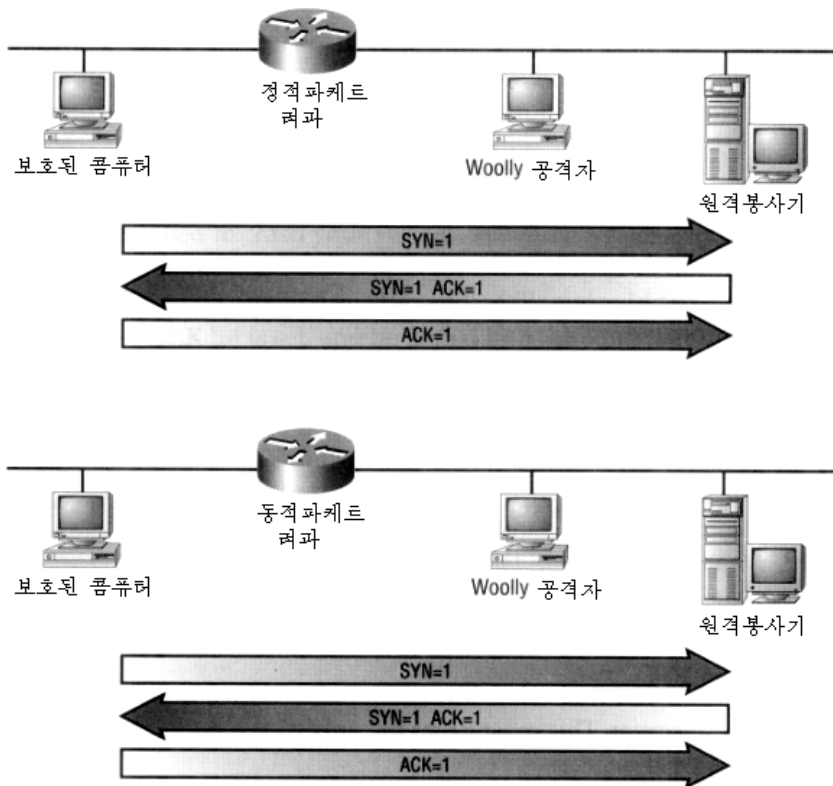



그림 5-6. 보호된 호스트로부터의 련결설정

그림 5-6에서 내부체계는 원격봉사기와의 하나의 통신대화를 설정하려고 하고 있다. 모든 통과하는 자료흐름은 접근조종목록에 설정된 기준을 만족시키므로 두 방화벽들은 이 자료흐름들을 통과시킨다.

일단 련결신호가 완성되면 보호된 호스트는 하나의 자료요청을 만든다. 이 파케트는 ACK비트가 설정되여 있고 PSH비트도 설정되여 있을수 있다. 원격봉사기가 이 요청을 받으면 그것도 ACK비트를 설정하고 가능하게 PSH비트도 설정하여 응답할것이다. 일단

자료전송이 끝나면 그 대화는 닫기고 매 체계는 FIN비트를 설정한 하나의 파케트를 전송하게 된다.

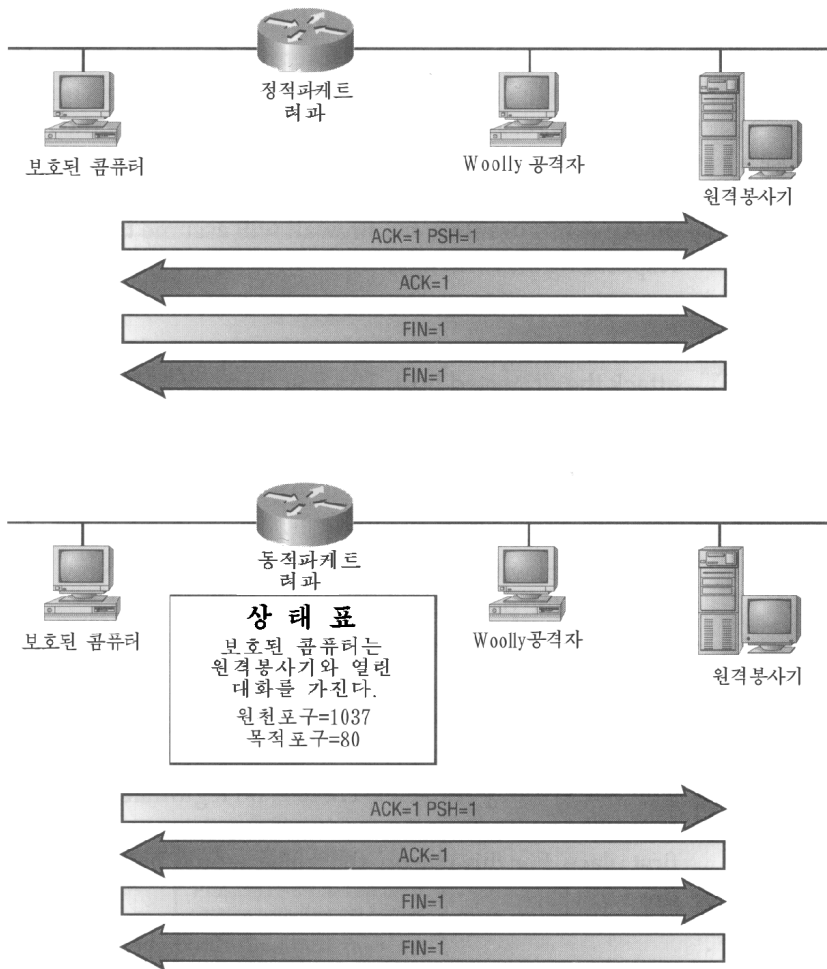



그림 5-7. 두 호스트사이에서 확립된 대화

그림 5-7은 이 설정된 대화가 자료를 통과시키는것을 보여 준다. 두번째 규칙 즉 《이미 설정된 임의의 대화는 통과시킨다.》에 의하여 방화벽을 통과하는데서 문제가 없다고 본다. 그러나 매개 방화벽은 이 결정을 하는데서 약간의 차이를 가지고 있다.

정적파케트려과기는 기발마당을 조사하여 SYN비트만이 1인가를 알려고 한다. 그렇게 되여 있지 않으므로 정적파케트려과기는 이 자료가 설정된 대화의 부분이라고 가정하고 그것을 통과하도록 한다.

동적파케트려과기는 같은 검사를 하고 있지만 그것은 련결이 처음으로 설정되였을 때에는 하나의 상태표항목을 만든다. 원격봉사기가 보호된 호스트에 응답하려고 할 때마다 상태표를 참조하여 다음의 내용을 담보하게 된다.

- 보호된 호스트가 하나의 자료요청을 실제로 만들었다.
- 원천포구정보는 자료요청과 맞는다.
- 목적지포구정보는 자료요청과 맞는다.

또한 동적파케트려과기는 순서번호와 답례번호도 다 맞는가를 확인할수 있다. 이 모든 자료가 정확하다면 동적파케트려과기는 그 파케트를 통과하도록 한다. 매 체계에서 FIN파케트가 전송되면 그 상태표항목은 제거된다. 또한 만일 일정한 시간동안(구성에 따라서 1min이나 지어 1h동안) 응답이 접수되지 않으면 방화벽은 그 원격봉사기가 더는 응답하지 않고 있다고 판단하고 그 상태표항목을 다시 지운다. 이것은 현재의 상태표를 그대로 유지한다.

이제 공격자가 이 자료흐름을 눈치 채고 그 보호된 호스트를 공격하기로 결심하였다고 하자. 그가 하려고 하는 첫째 일은 보호된 체계를 포구주사하여 그것이 어떤 듣는 봉사를 가지고 있는가를 알아 내는것이다. 그림 5-8에서 볼수 있는바와 같이 이것은 두 방화벽장치들이 다 막을수 있다. 그것은 초기주사하는 파케트들은 SYN비트가 1로 설정되여 있고 다른 모든 비트는 0이기때문이다.

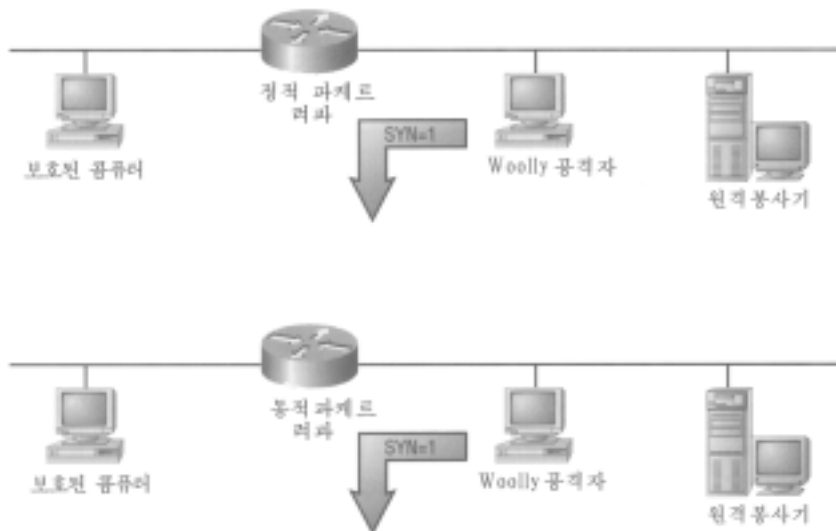



그림 5-8. 두 려과방법은 포구주사를 막을수 있다.

실망하지 않고 공격자는 ACK와 FIN비트가 1인 파케트를 전송함으로써 FIN주사를 하려고 시도한다. 이제 그 결과는 좀 다르다. 파케트려과기는 그저 SYN비트가 1인것을 찾고 있으므로 이 조건이 성립안되는것을 보고는 이 자료흐름을 쉽게 통과시키게 된다.

그러나 동적파케트려과기는 좀더 까다롭다. 그는 SYN비트가 설정되여 있지 않다는것을 알고는 이 자료흐름을 상태표와 비교하기 시작한다. 이 점에서 그는 우리의 보호된 호스트가 공격자와 결코 통신대화를 설정하지 않았다는것을 알게 된다.

우리의 호스트가 먼저 하지 않았다면 공격자가 하나의 대화를 끝내려고 할 아무러한 리유도 없다. 그러므로 이 자료흐름은 통과하지 못한다. 이것을 그림 5-9에서 보여주었다.

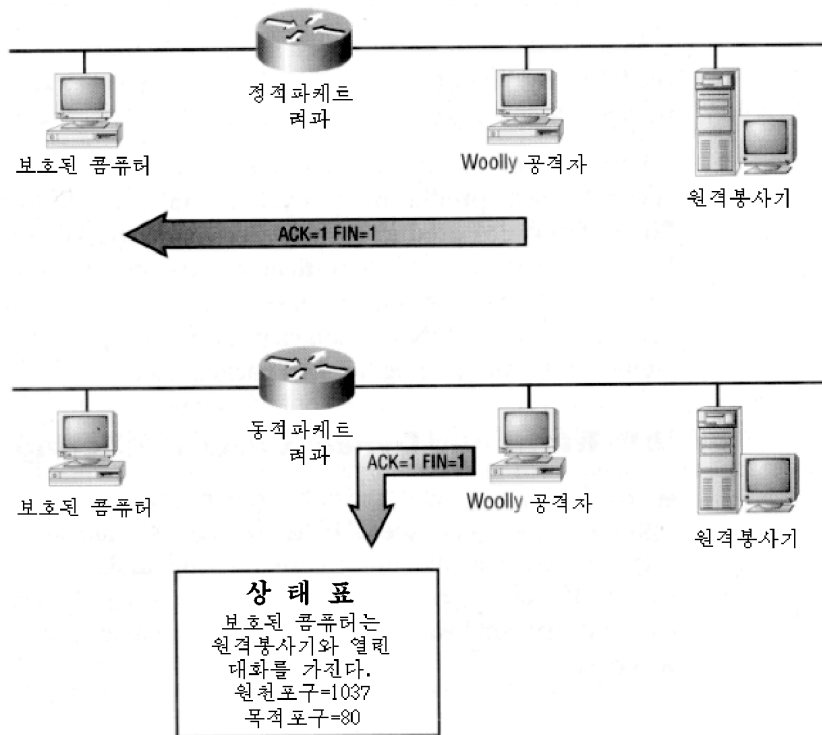



그림 5-9. FIN주사를 진행한 결과

그러면 만일 공격자가 원격봉사인것처럼 가장하여 방화벽을 속이려고 한다면 어떻게 되겠는가? 그가 이 공격을 성과적으로 수행하자면 많은 조건들이 갖추어져야 한다.

- 공격자는 원격봉사기의 IP주소를 속이거나 가정하여야 한다.
- 주소가 가정되였다면 공격자는 더 측정을 하여 원격봉사기가 스스로 요청들에 응답할수 없다는것을 확인하여야 한다.
- 주소를 속였다면 공격자는 도선에 붙지 않고 응답들을 읽는 어떤 방법을 가지고 있어야 한다.
- 공격자는 리용하고 있는 원천 및 목적지봉사포구들을 알아 냄으로써 자기의 자료흐름이 상태표의 그 항목들과 맞도록 하여야 한다.
- 실현방법에 따라 답례 및 순서번호들도 맞아야 한다.
- 공격자는 방화벽과 보호된 호스트에서의 시간초과를 피하기 위하여 충분히 빨리 통신대화를 처리하여야 한다.

이러한 공격을 가하는것은 가능하지만 성공하기는 쉽지 않다. 명백히 공격자는 지식이 매우 많아야 하며 이 모든 노력에 의하여 많은것을 얻으리라고 생각하여야 한다.

이러한 론의는 다만 리론적인것이라는것을 알아야 한다. 특정의 방화벽제품을 가졌을 때의 실제적인 정황은 달라 질수 있다. 실례로 이 책을 쓰는 기간에도 Check Point의 방화벽-1이라는 제품(이것은 동적파케트려과기이다.)이 많이 선전되였는데 그 내용은 규칙모임이 변화된후에도 상태표가 유지되게 한다는것이였다.

그런데 이 특징은 또한 상태가 항상 그렇게 효과적으로 유지되지는 않는다는것도 의미하고 있다. 방금 서술된 FIN주사식공격에서 Check Point의 방화벽-1은 주사파케트들까지 통과시켰다.

UDP자료흐름과 동적파케트려과

앞에서 본것처럼 정적파케트려과는 UDP자료흐름의 취급과 관련하여 몇가지 실제적인 문제들을 가지고 있다. 그것은 UDP머리부가 련결상태에 대해서는 정보를 가지고 있지 않기때문이다. 그러므로 동적파케트려과가 매우 유용한것으로 되고 있는데 여기서는 방화벽자체가 상태정보를 기억할수 있는것이다. 그것은 파케트머리부안에 있는 정보에 의거하는것이 아니라 모든 대화들의 상태와 관련하여 자기의 표를 가지고 있다.

일러두기

UDP자료흐름을 통과시키려고 할 때에는 정적려과가 아니라 동적려과를 사용할것을 강하게 권고한다. 상태표정보를 추가함으로써 이 방화벽방법은 봉사에서 손실 보는것보다 보안을 훨씬 더 강화하였다.

망의 전송층규약이 지원되는가

동적파케트려과의 실현은 전송층규약에 따라 다르다. 그것은 TCP, UDP 그리고 ICMP와 같은 매 전송층규약에 대하여 특징적으로 실현되여야 한다는것을 의미한다. 동적파케트려과기를 선택할 때 그 방화벽이 자기가 리용하려 하는 모든 전송층규약들에 대하여 상태를 유지할수 있는가를 확인해 보아야 한다.

실례로 방화벽-1의 판본 1.x에서 상태는 다만 UDP자료흐름에 대해서만 유지되였다. 그리고 TCP와 ICMP는 정적파케트려과와 같은 방법으로 처리되였다. 판본 2.x가 나와서야 TCP자료흐름에 대하여서도 상태가 유지되였다.

동적파케트려과에 대한 요약

동적파케트려과기는 파케트속성과 상태표에 기초하여 자료흐름조종결정을 만드는 지능적인 장치이다. 상태표가 있음으로 하여 방화벽장치는 이전의 통신파케트교환을 《기억》하고 이 보충적인 정보에 기초하여 판단을 하게 되는것이다.

동적파케트려과기의 가장 큰 제한성은 그것이 파케트안에 포함된 실제자료인 유효내용에 기초한 려과결정을 할수 없는것이다. 유효내용에 따라 려과하기 위하여서는 대리자에 기초한 방화벽을 리용하여야 한다.

상태려과

상태려과는 동적파케트려과의 능력을 개선한다. 처음에는 《여러준위상태검사》라는 이름으로 Check Point에 의하여 실현되였는데 상태규칙들은 규약에 따라 다르며 대화(상태가 아니라)의 문맥을 계속 기억하고 있다. 이것은 려과규칙들로 하여금 비련결성특성으로 하여 이전에 정적려과에서는 관리에서 면제되고 동적려과에서는 유일하게 식별되지 못하였던 여러가지 무접속형규약들(UDP, NFS 그리고 RPC와 같은)을 구별할수 있게 한다.

상태려과가 동적려과에 제공되는 가장 큰 보충은 련결상태가 아니라 응용프로그람상태를 유지하는 능력이다. 응용프로그람상태는 이전에 인증된 사용자가 재위임이 없이 새로운 련결을 만들수 있게 허용한다. 또한 련결상태는 하나의 대화기간 그 권한을 유지한다.

이것의 한가지 실례는 사용자인증에 기초한 내부접근을 허용하는 방화벽이다. 만일 한 인증된 사용자가 다른 하나의 열람기를 열려고 한다면 동적려과경로기는 그 사용자에게 그의 통과암호를 요구할것이다. 그러나 상태려과는 이미 존재하는(그리고 동시에 발생하는) 련결은 그 같은 기계에 대하여 유지되고 있다고 인식하고 자동적으로 추가적인 대화를 허용한다.

대리자

대리자봉사기(때로 응용프로그람관문 또는 송달자라고도 한다.)는 두 망토막사이에서 자료흐름을 중개하는 응용프로그람이다. 대리자는 흔히 려과기대신으로 리용되여 자료흐름이 두 망사이에서 직접 통과되지 않도록 한다. 대리자가 중개자로 동작하면 원천 및 목적지체계들은 사실상 서로 련결되여 있지 않게 된다. 대리자는 모든 련결시도에서 중개자로 역할한다.

대리자가 어떻게 자료흐름을 통과시키는가

파케트려과기와 달리 대리자는 자료흐름의 경로를 지정하지 않는다.

사실상 적당히 구성된 대리자는 모두 경로조종기능을 가지고 있지 않다.

그 이름이 귀띔하는바와 같이 대리자는 방화벽의 매측의 매 체계를 맡아 보거나 또는 대변한다.

한가지 비유로써 언어번역기를 통하여 말하고 있는 두 사람을 생각해 보자. 이 두 사람이 회화를 하고 있는것은 사실이지만 그들은 사실상 서로에게 말하고 있는것이 아니다. 모든 통신은 다른쪽으로 통과되기전에 번역기를 거치게 된다. 번역기는 리용된 언어의 일부를 씻어 내거나 또는 적대적이라고 느껴 지는 말들은 려과해 버릴수 있다.

이것이 어떻게 망통신과 관련되겠는가를 알기 위하여 그림 5-10을 보기로 하자. 내부호스트는 원격봉사기로부터 하나의 Web페지를 요청하려고 한다. 그것은 그 요청을 형식화하고 그 정보를 원격망을 이끄는 관문에로 전송한다. 이 경우에 관문은 대리자봉사

기이다.

대리자가 그 요청을 받으면 그것은 내부호스트가 어떤 형태의 봉사에 접근하려고 하는가를 식별한다. 이 경우에 호스트는 Web페지를 요청하였으므로 대리자는 그 요청을 HTTP대화를 처리하는데 리용되는 응용프로그람에로 보낸다. 이 응용프로그람은 HTTP 통신을 취급하는 하나의 기능을 가지고 기억기에서 돌아 가는 하나의 프로그람이다.

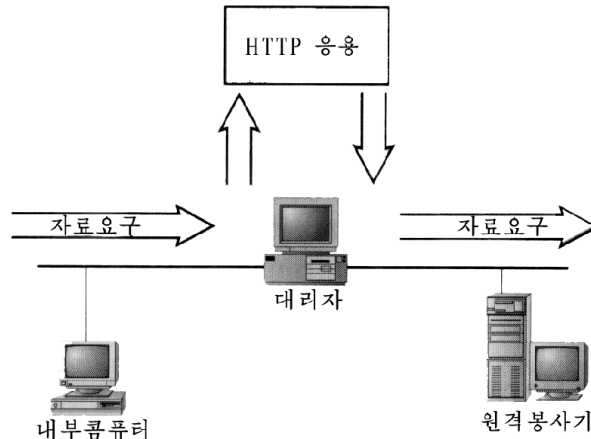



그림 5-10. 통신대화를 중개하는 대리자

HTTP응용프로그람이 이 요청을 받으면 그것은 ACL이 이러한 형식의 자료흐름을 허용하는가를 확인한다. 자료흐름이 허용된다면 대리자는 원격봉사기에 보낼 하나의 새로운 요청을 형식화한다. 이때 그것은 원천체계로서 자기자신만을 리용한다. 다른 말로 하면 대리자는 그 요청을 간단히 통과시키지 않고 원격정보를 위한 하나의 새로운 요청을 만드는것이다.

이 새로운 요청은 다음에 원격봉사기에 전송된다. 요청이 망분석기에 의하여 검사되면 그것은 내부호스트가 아니라 대리자가 그 HTTP요청을 만드는것으로 본다. 그러므로 원격봉사기는 대리자봉사기에로 응답하게 된다.

대리자봉사기는 응답을 받으면 그 응답을 또 HTTP응용프로그람에 보낸다. 그러면 HTTP응용프로그람은 원격봉사기가 보낸 자료를 비정상이 없는가를 세밀히 검토한다. 만일 자료가 접수가능하다면 HTTP응용프로그람은 하나의 새로운 파케트를 만들어 그 정보를 내부호스트에 전송한다.

알수 있는것처럼 두 끝체계는 사실상 직접적으로 정보를 교환하지 않는다. 대리자는 부단히 대화에 끼여 들어 그것이 다 안전하다는것을 확인한다.

대리자는 리용되고 있는 응용규약을 《리해》하여야 하므로 그들은 규약과 관련한 보안을 실현할수도 있다. 실례로 내부FTP대리자는 외부체계에 의하여 수신되는 Put와 mput요청들을 모두 려과해 내도록 구성될수 있다. 이것은 읽기전용FTP봉사기를 만드는데 리용될수 있다. 방화벽밖의 사람들은 FTP봉사기에 파일쓰기를 요구하는 명령을 보낼수 없다. 그러나 그것들은 FTP봉사기로부터 파일을 수신하게 하는 파일얻기명령을 수행할수 있다.

일러두기

대리자봉사기는 응용프로그람에 따라 다르다. 대리자를 통하여 새로운 규약을 지원하도록 하기 위하여서는 그 규약을 위한 대리자가 개발되여야 한다. 만일 대리자방화벽을 선택한다면 그것이 자기가 리용하려고 하는 모든 응용프로그람들을 지원하는가를 확인하여야 한다.

꽂개식관문(plug gateway)이라고 부르는 간단한 대리자도 있다. 그것들은 지원하는 응용프로그람을 리해하지 않으므로 진짜대리자라고는 말할수 없다. 꽂개식관문은 그저 특정의 봉사포구를 위한 련결성을 제공하며 동적려과보다 더 큰 리득을 주는것은 없다.

대리자환경에서 의뢰기구성

어떤 대리자봉사기들은 모든 내부호스트들이 SOCKS나 변경된 winsock.dll파일과 같은 련결쏘프트웨어를 돌릴것을 요구한다. 이 매 프로그람은 하나의 기능을 봉사한다. 즉 모든 비국부적자료흐름을 대리자에게로 전송한다. 환경에 따라 이것은 매우 리롭거나 또는 아주 나쁘게 될수도 있다.

대리자의뢰기의 우점

대리자의뢰기쏘프트웨어를 돌리면 많은 우점이 있다. 첫째는 구성이 쉬운것이다. 의뢰기는 모든 비국부자료요청들을 대리자에게 보내도록 설계되므로 유일하게 요구되는 구성정보는 유효한 IP주소들과 부분망마스크이다. 경로기와 DNS파라메터들은 무시될수 있다. 그것은 이 정보가 대리자우에서 구성될 때에만 필요하기때문이다.

사실상 많은 대리자들은 통신규약으로 IP를 리용할것조차 요구하지 않는다. 실례로 Microsoft대리자봉사기2.0은 하나의 교체winsock.dll파일을 가지고 있는데 그것은 IPX가 국부워크스테이션에 리용되도록 허용한다. 일단 자료흐름이 대리자에게 도달하면 그것은 IP로 변환되여 원격봉사기에 전송된다. IPX가 지배적인 환경에서 이것은 망에 추가적인 규약을 돌릴것을 피할수 있는 매우 간단한 방도로 될수 있다.

대리자의뢰기는 둘째로, 가입이름과 통과암호에 기초한 외부련결시도를 허가하기 위하여 투명한 인증을 제공한다. 실례로 노벨의 BorderManager는 NetWare등록부봉사(NDS)와 결합되여 사용자가 인터네트에 접근할 때 그것을 투명하게 인증한다. 사용자가 NDS에 인증되는 한 그 사용자는 인터네트자원에 접근할 때 통과암호를 넣지 않아도 된다.

주 의

바깥방향대화의 사용자인증은 증가된 가입등록과 관리를 위하여 리용된다. 인증이 리용되지 않는다면 방화벽은 원천IP주소에 의거하여 누가 어느 인터네트자원에 접근하였는가를 식별하여야 한다. 이것은 하나의 문제로 될수 있다. 자기의 신원을 변경시키려면 사용자는 자기의 IP주소를 변경시켜야 한다. 이것은 DHCP 또는 Bootp환경에서 자기의 모든 사용자들을 추적하려고 한다면 심중한 문제로 될수 있다.

대리자의뢰기의 부족점

대리자의뢰기를 리용하는데는 많은 부족점도 있다. 우선 배비이다. 만일 대리자봉사기를 리용하려고 하는 1000개의 기계를 가지고 있다면 이 매 기계들에 보충적인 쏘프트웨어를 적재하여야 한다. 쏘프트웨어호환성도 문제로 된다. 어떤 응용프로그람들은 교체 winsock.dll와 호환가능하지 않다. 실례로 Winsock2.x를 요구하는 응용프로그람들이 지금 있음에도 불구하고 많은 Winsock교체프로그람들은 아직 1.x명세로 작성되고 있다.

그러면 많은 탁상콤퓨터들이 Windows를 돌리지 않는다면 어떻게 될것인가? 많은 대리자들은 Windows가 아닌 조작체계에 대한 의뢰기쏘프트웨어를 제공하지 않는다. 이 경우에는 자기가 리용하려고 하는 모든 IP응용프로그람들이 SOCKS호환인가를 확인하여야 한다. TELNET와 FTP와 같은 많은 IP응용프로그람들의 SOCKS판이 있으나 좋아 하는 응용프로그람이 SOCKS호환이 아닌것은 유감스럽게도 흔히 있는 일이다.

의뢰기쏘프트웨어도 이동사용자 또는 휴대형콤퓨터사용자들에게 있어서 문제로 된다. 실례로 한 휴대용콤퓨터사용자가 낮에는 국부망에 련결하고 밤에는 자기의 인터네트봉사제공자(ISP)에 전화접속한다고 하자. 이 경우에 그는 자기의 대리자의뢰기가 낮에는 쓸수 있지만 밤에는 쓸수 없다는것을 알아야 한다.

마지막으로 대리자의뢰기는 당신이 여러개의 망토막들을 가지고 있다면 실제적인 문제로 될수 있다. 이것은 대리자의뢰기가 모든 비국부자료흐름을 대리자봉사기에 전송할것을 기대하고 있기때문이다. 이것은 만일 많은 부분망들을 가지는 큰 망환경을 가지고 있다면 좋은 해결책이 못된다. 어떤 구성에서는 일정한 부분망들을 대리자에게 자료전송하는데서 면제시키게 하고 있으나 이것은 국부워크스테이션에 보관된 본문파일을 변경시킬수 있다.

다시 만일 1000개의 탁상형콤퓨터를 고려하고 있다면 부분망주소변화에 따라 그것들을 갱신하기 위하여 며칠밤을 새워야 할것이다.

투명한 대리자

모든 대리자들이 특수한 의뢰기쏘프트웨어를 요구하는것은 아니다. 일부는 투명한 대리자로서 동작할수 있는데 그것은 모든 내부호스트들이 대리자가 마치도 인터네트에 련결하는 보통의 경로기인것처럼 구성된다는것을 의미한다. 대리자가 자료흐름을 받을때 그는 그것을 그림 5-10에서 본 실례와 류사한 방법으로 처리한다.

만일 대리자방화벽이 자기의 보안요구에 가장 잘 맞는다고 결심한다면 또한 투명대리자를 리용할것인지 아니면 비투명대리자를 리용할것인지를 결정하여야 한다. 많은 대리자프로그람묶음에 대한 시장자료는 그것이 특수한 의뢰기쏘프트웨어를 요구하는가에 대하여 좀 애매하다. 대표적으로 한 제품이 SOCKS를 지원한다고 주장한다면 그것은 투명대리자가 아니다. 그러므로 방화벽문제에 투자하기전에 그 요구를 알아야 한다.

Java, ActiveX 및 HTML스크립트들의 려과

아는바와 같이 대리자들은 자료파케트의 유효내용을 분석하고 이 파케트를 통과시킬것인가 떨굴것인가를 결정할수 있다. 이것은 관리자로 하여금 어떤 형식의 자료가 망에 허용되여야 하는가를 세심히 분석할수 있는 강한 능력을 가질수 있게 하는 좋은

특징이다. 내용려과를 고찰할 때 대부분의 사람들이 먼저 생각하는것은 Java와 ActiveX이다.

Java는 이식성 있는 프로그람언어이다. 이식성이란 그것이 임의의 망조작체계상에서 돌수 있도록 설계되였다는것을 의미한다. 대표적으로 Java지원은 Java지향Web열람기의 리용을 통하여 실현된다. Java프로그람을 애플레트(applet)라고 부른다.

ActiveX는 Microsoft의 대상련결 및 매몰(OLE) 또는 요소대상모형(COM)개체의 전문화된 실현이다. ActiveX에 의하여 ActiveX Control이라고 부르는 자급자족형프로그람을 만들수 있다.

ActiveX Control의 리점은 그것이 여러 응용프로그람들에 공유될수 있다는것이다. ActiveX는 프로그람언어는 아니다. ActiveX Control은 C++, PowerBuilder, Visual Basic 또는 Microsoft Java와 같은 다른 프로그람언어들을 리용하여 만든다.

Java애플리트와 ActiveX Control은 봉사기로부터 가져 와서 어떤 호환가능한 Web열람기에서 돌릴수 있다. 이 프로그람들의 기능은 춤추는 아이콘으로부터 공유된 응용프로그람까지 많은것을 포함한다. 만들어 질수 있는 프로그람의 형식에는 얼마간 제한이 있다.

이로 하여 문제가 시작된다. Java와 ActiveX는 둘 다 보안을 고려하여 개발되였지만 (Java가 ActiveX보다 더 강하다.) 몇가지 보안상 약점이 발견되였다.

주 의

보안상 약점들의 종류를 보려면 Web열람기로 www.digicrime.com을 찾으시오. 이 싸이트에는 많은 Java 및 ActiveX 약점들이 포함되여 있으며 이 프로그람들이 나쁜 손에 들어 가면 얼마나 위험한가를 보여 준다.

Java와 ActiveX를 리용하는것이 그리 좋지 않다고 생각한다면 문제는 그에 대처하여 무엇을 할수 있는가 하는것이다. 많은 대리자방화벽들은 Java와 ActiveX프로그람코드들의 전부 또는 일부를 려과해 낼수 있는 능력을 제공한다. 이로 하여 망사용자들은 나쁜 응용프로그람을 돌린다는 생각을 하지 않고 계속 원격Web싸이트들을 접근할수 있다.

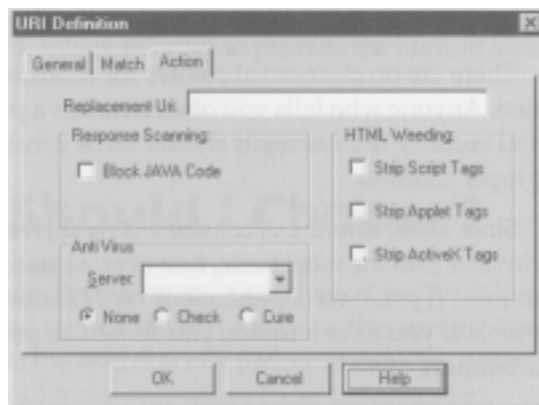



그림 5-11. 프로그람코드를 려과하게 하는 URI정의대화칸

실례로 방화벽-1은 보안봉사기라고 부르는 대리자응용프로그람을 가지고 있다. 보안봉사기는 방화벽관리자에게 그가 려과하려고 하는 일정한 프로그람코드들을 식별하는 능력을 준다. 그림 5-11은 방화벽-1관리자에게 그가 려과하려고 하는 코드형태들을 골라낼수 있게 하는 URI대화칸를 보여 준다.

HTML Weeding검사칸은 관리자로 하여금 Java 스크립트, Java 애플리트 또는 지어 ActiveX Control에 대한 모든 꼬리표참조를 려과하게 한다.

Block Java Code검사칸은 방화벽이 모든 Java프로그람코드를 려과하게 한다. 이 선택들의 결합은 어떤 형태의 자료들을 내부Web열람기에 도달하게 할것인가를 결정하는데서 어떤 유연성을 제공한다.

주 의

이 특징들을 가능으로 하면 좋은것과 나쁜것을 구별하지 않고 다 막는다. 다른 말로 하면 당신의 선택은 전체 또는 아무것도 없을수 있다. 그러나 《나쁜 프로그람코드》라고 알려 진것만 선택적으로 려과해 내는 대리자들이 있다. 이것은 Java나 ActiveX가 그 대리자에로 통과하게 하지만 그것은 낮은 보안수준에서 그렇게 한다. 이 대리자들은 알려 진 문제들만 려과할수 있다. 이것들은 아직 발견된 약점들을 보강할수 없다. 가장 최근의 약점들에 머무르고 있지 않는 한 아직은 자기의 방화벽을 나쁜 코드들이 통과하는것을 막을수 있다.

어떤 류형의 방화벽을 리용하여야 하는가

이 절의 제목은 많은 뜻이 담긴 질문으로 되여 있다. 이 질문을 방화벽토론에 제시한다면 분명 격렬한 론쟁들이 시작되게 될것이다(이 물음뒤에 다음과 같은 질문을 덧붙이는것이 좋다. 《나의 방화벽을 마킨토쉬, Unix, Linux, NT, Windows 2000 또는 제작자에 따르는 플래트홈에서 돌려야 하는가?》).

특정의 방화벽형태를 선택하는데서 명백하고 절대적인것은 없다. 다르게 말하는 사람이 있다면 그것은 자기의 제품을 실현하려고 그러는것이다. 비용, 기업상의 필요 그리고 보안요구 등은 적당한 해결책을 찾고 있을 때 꼭 고려되여야 할 문제들이다.

정적려과는 약하다고 생각되므로 그것은 경계선보안의 가장 낮은 수준이다. 그러나 정적려과능력은 대부분의 경로기들에 준비되여 있으므로 이것은 가장 기초적인것으로 된다. 만일 영구적인 WAN련결을 가지고 있다면 경로기를 리용할수 있다. 경로기를 가지고 있다면 최소로 정적파케트려과를 수행하고 있어야 한다.

동적려과 또는 대리자

이 매개 방화벽들은 자기의 장점과 약점을 가진다. 동적려과는 대리자보다 일하기 더 쉽고 대부분의 기업요구에 더잘 맞는 능력을 가지고 있지만 대리자봉사기와 같이 그렇게 세밀하게 골라 내는데서는 유능하지 못하다. 동적파케트려과와 대리자는 둘다 나쁘다고 알려 진 자료흐름을 차단하지만 애매한 자료에 대하여서는 매개가 약간 다르게 동

작한다.

실례로 두개의 방화벽 즉 동적파케트려과기와 대리자를 가지고 있다고 하자. 그 매개는 일정한 응용프로그람에 대하여 높은 우선권기발설정을 가지는 하나의 자료파케트를 수신하는데 이러한 형식의 자료를 어떻게 처리할것인가에 대하여서는 서로 다르게 프로그람화되였다. 대표적으로(그러나 항상은 아니다.) 동적파케트려과기는 문제의 자료흐름을 통과시키며 대리자는 그것을 떨군다. 또한 대리자는 응용프로그람지향이므로 실제자료의 내용을 더 검열하지만 동적려과기는 그렇게 할수 없다. 이것은 경계선보호의 두가지형태에 대한 리론적비교이다. 실제적인 과정은 선택하는 구체적인 제품에 따라 변할수 있다.

대리자는 좀더 안전하지만 그것들은 특정의 기업요구에 맞추는것이 보다 어렵다. 실례로 많은 대리자들은 Microsoft의 NetMeeting이나 Real Audio와 Video와 같은 현대적인 봉사들을 지원하는데서는 좀 불편하다. 그러므로 경계선보안의 수준은 더 높지만 대리자가 그것이 보호하는 기관의 기업요구를 맞출수 없다면 그것은 즐겁지 못한것이다.

가장 안전한 경계선보안장치는 한쌍의 도선절단기이다. 적당한 방화벽선택은 가장 높은 보안수준을 가능하게 하면서 련결성에 대한 기업요구를 모두 만족시키는것이다. 보충으로 말하면 좋은 방화벽제품은 가장 높은 보안수준과 유연성을 제공하기 위하여 동적파케트려과와 대리자기술을 결합한것이다.

어느 플래트홈을 선택하여야 하는가

적당한 방화벽플래트홈의 선택은 적당한 연구가 끝난 다음에야 만들어야 할 개인적인 결심이다.

이 절에서는 독자들에게 어느 플래트홈을 선택하라고 말하려고 하지 않는다. 여기서는 그저 매 플래트홈의 장점과 약점들을 지적하며 최종적인 결정은 독자에게 남겨 둔다. 적당한 방화벽제품을 선택하는것과 마찬가지로 그것을 돌릴 조작체계를 선택하는것도 명백히 하나로 모든것을 맞추는 관점으로는 되지 않는다.

봉사기에 기초한 방화벽과 응용에 기초한 방화벽사이에는 한가지 중요한 차이가 있다. 봉사기에 기초한 방화벽은 조작체계우에서 돌아 가는 응용프로그람이다. 한가지 실례는 Check Point의 방화벽-1인데 그것은 Windows NT와 2000에서 돌아 간다. 응용에 기초한 방화벽 또는 집적방화벽은 전용하드웨어 또는 쏘프트웨어에서 돌아 가는 방화벽응용프로그람이다. 실례로 Cisco PIX방화벽이 집적장치의 한 실례인데 여기서 전체 체계는 방화벽이 아닌 다른 일은 할수 없고 봉사기의 전통적인 구성부분들이나 하드구동기도 가지고 있지 않다. 그것의 집적성과 전용적인 특성으로 하여 이 장치들은 봉사기에 기초한 방화벽보다 전통적으로 더 빠르고 더 믿음직하며 더 안전한것으로 평가되고 있다. 한편 봉사기에 기초한 방화벽들은 흔히 추가적인 구성을 제공하고 선택을 지원하며 집적화방법보다 더 눅을수 있다.

봉사기에 기초한 방화벽

봉사기에 기초한 방화벽은 어떤 조작체계우에서 돌아 가는 응용프로그람들이다. 다음과 같은 플래트홈들에서 돌아 가는 방화벽들이 있다.

- 마킨토쉬(Macintosh)
- 유닉스(UNIX)
- 리눅스(Linux)
- Microsoft Windows NT
- Microsoft Windows 2000

마킨토쉬

대부분의 체계관리자들에게는 그렇게 될것 같지 않아 보이지만 마킨토쉬조작체계를 위하여 설계된 방화벽제품들이 있다. 그리고 어떤 체계관리자들은 그 생각을 비웃을수도 있지만 마크(Mac)에 기초한 안전한 인터네트체계들에 대한 인상적인 실례들도 있다. 실례로 미군은 1999년초부터 마킨토쉬OS에서 동작하는 WebSTAR봉사기에서 자기의 Web싸이트를 운영하고 있는데 그 봉사기는 그이후 해킹 당한적이 없다고 한다.

그러나 마킨토쉬조작체계는 근본적인 변화를 겪고 있으며 그것은 2001년에 OS X(10)이라는 소비자판본을 출하하고 끝나게 되여 있다. OS X는 NeXTStep조작체계에 기초하고 있는데 그자체는 마크의 핵과 BSD(유닉스의 Berkeley SoftWare Distribution)에 기초하고 있다. Apple은 OS X의 원천코드를 공개하였지만 그것은 그 핵을 마킨토쉬플래트홈에 적응시키도록 하는 중대한 변화를 가져 왔다. 이 변화들(DNS와 HTTP의 Apple에 의한 실현에 따르는)이 전체로서 보안에 어떤 영향을 미칠것인가 하는것은 아직 두고 보아야 한다.

마킨토쉬의 우점 그러면 조작체계로서의 마킨토쉬를 다른 주목되는 봉사기 OS들과 구별하게 하는것은 무엇인가? 대부분의 해커들이 마크의 기술을 잘 모르기때문에 마크우에서 방화벽을 돌리는것은 보다 안전할것이라는 일반적인 믿음이 존재하고 있다. 그리고 마크우에서 돌아 가는 응용프로그람들에 대해서는 몇가지 취약점들이 보고되고 있으나 조작체계자체에 대해서는 약점에 대한 기록자료가 매우 적다.

또한 구성이 쉽다는것도 있다. 마킨토쉬는 GUI에만 기초하고 있고 매우 적은 망봉사를 제공하므로 복잡성은 크게 감소된다.

마지막으로 새로운 OS X에서 돌아 가는 방화벽은 성능에서(최첨단의 UNIX에 기초한 조작체계로부터), 구성에서(매개의 특정의 봉사는 마음대로 켜거나 끌수 있다.) 그리고 지원도구에서(대부분의 UNIX에 기초한 보안지원도구들이 OS X에서도 돌아 간다.) 우점을 보여 주고 있다.

마킨토쉬의 약점 마킨토쉬의 우점의 뒤면들로 되는 몇가지 중요한 약점들이 존재한다. 이 체계는 잘 알려 져 있지 않기때문에 많은 취약점들이 그것에 침투하려는 엄중한 시도를 하고 있는 해커에 의하여 발견될수 있는 가능성이 있다.

또한 마킨토쉬봉사기는 제한된 수의 구성과 응용프로그람선택만을 가지고 있으므로

관리자들은 그것이 봉사기에서 구성요소들을 자유롭게 선택하는것과 같은 나머지 문제들을 놓치고 있다고 느낄수 있다.

그리고 마킨토쉬를 위한 방화벽제품들이 있지만 그 대부분은 개인용방화벽으로 설계되고 전체 망을 보호하는 봉사기로는 기능하지 않는다. 이것은 방화벽을 위한 많은 봉사도구들이(마킨토쉬에 기초한 분석 및 응답도구들) 없는것으로 하여 마킨토쉬방화벽의 유연성을 더 크게 제한한다.

성능상에서도 문제가 있다. 최근년간에 Apple의 하드웨어는 매우 인상적인 성능을 보여 주었지만 조작체계는 그에 따르지 못하고 있다. 결과로 방화벽과 경로기로 동작하는 매우 나쁜 마킨토쉬봉사기는 점차 압도될수 있다.

게다가 OS X는 몇가지 새로운 약점들을 끌어 들이였다. 그것은 UNIX를 계승하고 있으므로 OS X에서의 가장 큰 보안위험은 기정으로 설치된 데몬들(봉사들)에 의하여 일어 나게 된다. 그 일부를 우리는 다음에 UNIX를 취급할 때 구체적으로 보기로 한다.

UNIX

UNIX는 Microsoft의 Windows NT(그리고 Windows 2000과 같이 NT에 기초한 조작체계들)도 포함하여 다른 조작체계들보다 매우 력사가 오래며 첫 방화벽은 UNIX체계우에서 설계되였다. 이것은 그우에서 돌아 가는 방화벽제품들이 안정할것이라는것을 의미한다. UNIX의 대부분의 판본들은 상업적으로 판매되였지만(Sun의 Solaris, HP의 HP-OX 그리고 IBM의 AIX) 많은 사람들이 그것의 기본구조와 봉사에 대하여 알고 있으므로 그것은 열린 체계로 간주되고 있다.

UNIX에서 보안약점들이 발견되였어도 그것들은 핵심조작체계와 관련된것이 아니고 그우에서 돌아 가는 응용프로그람이나 봉사와 관련된것들이였다.

UNIX는 또한 다른 조작체계를 릉가하는 우점을 가지고 있다. 이것은 많은 하드웨어 플래트홈과 UNIX를 지원하는 구성들과 결합되여 UNIX를 집중적이고 큰 자료연산을 위한 가장 적합한 조작체계로 되게 하고 있다. 방화벽이 잘 동작하자면 그 방화벽의 동작에서 본질적이 못되는 모든 응용프로그람들과 구성요소들은 불가능하게 되여야 하는데 이것은 UNIX에서 특별히 실행하기 쉽다.

UNIX의 우점 UNIX의 고유한 우점들은 많다. 그것은 구성성이 매우 좋으며 보안산업분야의 많은 사람들에게 잘 리해되여 있고 현존하는 조작체계들중 가장 우수한것으로 되고 있다. 제기되는 보안문제들을 리해하고 개선하는데 많은 자원들이 투하되였다.

UNIX는 또한 매우 안정한 고성능조작체계로 인정되고 있다. 그리고 여러 하드웨어 플래트홈(DEC Alpha와 IBM RS/6000과 같은)들과 이 플래트홈의 다중처리판본들에서 돌아 갈수 있는 능력으로 하여 그것은 큰 망을 지원하는 방화벽들에 필요한 높은 자료속도를 지원할수 있다.

그것은 또한 Windows NT에 기초한 체계들을 괴롭히던 구성변화가 있은후 체계를 재기동하여야 하는 조작을 하지 않게 된다.

UNIX를 위한 보안 및 보안지원제품은 그 어떤 다른 플래트홈들에서보다 많다(Windows NT는 두번째이다.). 그러므로 이 사실과 30년의 력사로 하여 UNIX는 많은 큰 기관들에서 선택하는 우월한 조작체계로 되였다.

UNIX의 약점 그러면 결함은 무엇인가? 문제는 경험 없는 UNIX관리자들이 《칸밖의 설치》로 방화벽을 설치하고 기정에 의하여 가능으로 되는 많은 취약한(그러나 방화벽이 없는 체계에서는 잠재적으로 취약한) 프로그람들과 봉사들(데몬들)을 불가능으로 하지 않을 때에 제기된다. 또한 이 데몬들의 대부분이 뿌리(매우 강력한 초사용자권한)의 보안문맥에서 돌아 가도록 구성되였기때문에 그것들은 공격자에게 그들이 일단 취약한 구성을 리용한다면 체계에 완전히 접근할수 있는 가능성을 준다.

비활성데몬들은 비교적 간단하다. 관리자들은 기동시간에 각각의 데몬들을 활성화시키는 스크립트들을 제거 또는 이름바꾸기하거나 또는 그 데몬이 inetd에 의하여 호출된다면 inetd.conf구성파일에서 그 행을 설명문으로 만들어 버린다(inetd.conf구성파일을 참고하시오.).

inetd.conf구성파일은 다음과 같다.

```
# These are standard services.
ftp      stream tcp nowait root /usr/sbin/tcpd in.ftpd-1 -a
telnet   stream tcp nowait root /usr/sbin/tcpd in.ttlnetd
gopher   stream tcp nowait root /usr/sbin/tcpd gn
#smtp    stream tcp nowait root /usr/bin/smtpd smtpd
#nntp    stream tcp nowait root /usr/sbin/tcpd in.nntpd
#
# shell, login, exec and talk are BSD protocols.
#
shell    stream tcp   nowait root   /usr/sbin/tcpd in.rshd
login    stream tcp nowait   root   /usr/sbin/tcpd in.rlogind
#exec    stream tcp nowait   root   /usr/sbin/tcpd in.rexecd
talk     dgram  udp   wait   root   /usr/sbin/tcpd in.talkd
ntalk    dgram  udp   wait   root   /usr/sbin/tcpd in.ntalkd
#dtlk    stream tcp   waut   nobody /usr/sbin/tcpd in.dtalkd
#
#pop and imap mail services et al
#
pop-2    stream tcp   nowait root   /usr/sbin/tcpd in.ipop2d
pop-3    stream tcp   nowait root   /usr/sbin/tcpd in.ipop3d
imap     stream tcp   nowait root   /usr/sbin/tcpd imapd
#
#Tftp service is provided primarily for booting. Most sites
#run this only on machines acting as «boot servers.» Do not uncomment
#this unless you *need* it.
#
#tftp    dgram  udp   wait   root   /urs/sbin/tcpd in.tftpd
```

```
#bootps     dgram   udp     wait     root     /usr/sbin/tcpd  bootpd
#
#Finger, systat and netstat give out user information which may be
# valuable to potential «system crackers.» Many sites choose to disable
# some or all of these services to improve security
#
# cfinger is for GNU finger, which is currently not in use in RHS Linux
#
finger      stream  tcp     nowait   root     /usr/sbin/tcpd  in.fingerd
#cfinger    stream  tcp     nowait   root     /usr/sbin/tcpd  in.cfingerd
#systat     stream  tcp     nowait   guest    /usr/sbin/tcpd  /bin/ps-auwwx
#netstat    stream  tcp     nowait   guest    /usr/sbin/tcpd  /bin/netstat-finet
#
# Time service is used for clock synchronization
#
time        stream  tcp     nowait   nobody   /usr/sbin/tcpd  in.timed
time        dgram   udp     wait     nobody   /usr/sbin/tcpd  in.timed
#
# Authentication
#
auth        stream  tcp     nowait   nobody   /usr/sbin/in.identd  in.identd-1-e-0
#
# End of inetd. conf
```

한 주간을 보면 UNIX에서 어떤 다른 조작체계들보다 더 많은 약점들이 악용된다. 하나의 실례로 CERT(카네기멜론대학의 콤퓨터긴급응답기구)는 2000년 9월 15일에 발표하기를 해커들이 두가지의 취약성을 리용하여 넓은 범위의 공격을 진행하였다는것이다. 그 첫번째 취약성은 NFS(망파일체계)를 지원하는데 리용되는 데몬인 rpc.statd와 관련한것이다. 두번째는 워싱톤종합대학에서 제공한 ftp봉사기프로그람묶음인 wu-ftpd와 관련된것이다. 이 봉사들은 대부분의 UNIX(그리고 Linux)체계들에서 기정으로 설치되고 활성화되므로 기정설치로 방화벽을 설치하는 관리자는 자기의 전체 망을 취약하게 만들게 된다.

UNIX는 배우고 관리하기가 매우 어려운것으로 간주되고 있으며 UNIX체계의 가격은 다른 조작체계들보다 전통적으로 비쌌다. 또한 UNIX와 관련한 많은 약점들이 알려 져 있으므로 관리자는 체계를 안전하게 하는데 많은 시간을 들여야 한다. 그렇게 하지 않으면 UNIX의 취약점들에 대한 정보를 알고 있는 공격자가 이 많은 《구멍》들을 리용할수 있다.

OpenBSD: UNIX규칙의 한가지 례외 미리 설치된 취약한 데몬들의 위험을 최소화하는 한가지 UNIX변종이 있는데 그것은 OpenBSD이다. OpenBSD는 접근가능성없이 설치한다. 관리자가 수동적으로 어느 봉사와 구성부분들이 돌아 갈것인가를 선택하여야 한다.

OpenBSD는 자원봉사자들에 의하여 무료로 만들어 지고 유지되고 있는데 때로는 Linux와 혼돈된다. 사실상 그것은 특정의 목적을 가지고 매우 엄격히 조종되는 UNIX의 한가지 공동연구프로젝트이다. 아직 약점이 있을수 있지만 이 약점들을 수정하기 위한 응답시간은 산업계에서 가장 좋은것으로 간주되고 있다. 또한 쏘프트웨어오유들을 찾아내고 수정하는데서 혁신적인 사고방식으로 하여 OpenBSD는 많은 방화벽관리자들에게 있어서 거절하기 어려운 선택으로 되고 있다.

Linux

최근의 기록에 의하면 조작체계전쟁에서 가장 큰 도전인 Linux는 어떠한가? Linux는 UNIX와 많은 우점들과 약점들을 함께 가지고 있다.

Linux의 우점 UNIX와 마찬가지로 Linux는 구성성이 좋고 안정하고 잘 리해되며 많은 준비된 보안관련제품들을 가지고 있다. 그러나 Linux의 가장 큰 매력은 그것의 개발성이다. 사실상 Linux는 OpenBSD보다 더 열려 있으며 보안산업분야의 많은 사람들은 이것으로 하여 보다 많은 눈들이 오유와 취약성들을 찾아 내도록 하기 위하여 원천코드를 공개할수 있게 하는것이다. 그리고 Linux공동체의 특성은 보안전문가들에게서 관심과 문제점들을 가지고 있는 준비되고 자발적인 지원집단이라는것을 의미한다.

Linux의 약점 Linux의 약점은 배우기 어렵고 많은 알려 진 취약점들을 가지고 있다는것이다.

Microsoft Windows NT

Linux와 대조적으로 Microsoft는 친절하다는 우점을 가지고 있다. 그러나 쎄르반테스가 《돈 키호테》에서 쓴바와 같이 친절은 경멸을 낳으며 그것은 Microsoft Windows NT와 Windows 2000에 대해서도 마찬가지이다.

NT의 우점 Windows NT는 Windows Desktop 환경의 확장이므로 NT는 대표적인 말단사용자에게서 보다 친근한 환경이다. 이것은 그 사용자가 방화벽쏘프트웨어를 돌리기 위하여 새로운 환경을 완전히 배우지 않아도 된다는것을 의미한다. 보다 중요한것은 회사가 자기의 방화벽을 관리하기 위하여 추가적인 자원을 소비하지 않아도 된다는것이다.

사실상 NT에 기초한 체계들은 전통적으로 UNIX관련체계들보다 비싸지 않았으며 하드웨어와 쏘프트웨어에 대한 투자가 NT에 기초한 체계에서 보통 더 적다는 사실을 고려하여야 한다.

친절성은 보안을 강화한다고 말할수 있다. 사람들이 NT와 잘 알고 있기때문에 그것들이 플래트홈을 틀리게 구성하여 보안상 문제를 일으키는 일은 보다 적어 질것이다. UNIX가 보다 안전한 환경으로 구성될수 있다는것은 진실일수도 있고 아닐수도 있으나 확실히 사용자가 그것을 어떻게 적당히 관리할것인가를 리해하지 못한다면 안전한 환경은 결코 이루어 질수 없다.

마지막으로 중요한것은 일관성이다. 많은 기관들에서는 파일, 인쇄 및 응용프로그람봉사를 위하여 돌리고 있으므로 모든 입구되는 봉사들을 위하여 하나의 플래트홈으로 규격화하는것이 중요하다. 이렇게 하면 관리가 더 쉬워 지고 보다 조화롭게 된다. 또한 이것은 호환성문제를 약화시키거나 없애는데도 도움이 된다.

NT의 약점 NT의 가장 큰 약점은 인식상의 문제인데 즉 Microsoft가 보안약점을 인정하고 수정하는데서 매우 느리고 달갑게 여기지 않는다는것이다. 어떤 제3자가 하나의 약점을 발견하고 그것을 Microsoft에 남몰래 알려 준적이 있었다. 그런데 Microsoft는 한달이 지나도 그것을 수정하기 위한 패치프로그람을 발표하지 않고 전혀 움직이지도 않았으므로 그 사람은 그것을 일반에 공개하고 말았다. 중요한 취약점들이 발견되여도 그들은 대개 봉사를 NT에 미리 설치되여 있지 않았던것들에로 제한할뿐이다.

NT의 독점적인 성질로 하여 봉사의 내부적동작에 대하여서는 많은것들이 알려 지지 않고 있으며 UNIX데몬들과 같은 정도로 구성가능하지 못하다. 이것은 또한 자기들의 방화벽이 돌아 갈 가장 안전한 플래트홈을 찾고 있는 보안전문가들에게도 몇가지 불확실성을 주고 있다.

다른 결함들은 구성변화후에 NT봉사기를 재기동하여야 하는것과 NT봉사기와 관련한 구입 및 허가권료금 등의 문제이다.

Windows 2000

Windows 2000은 Windows NT와 어떻게 비교되는가? Windows 2000은 Windows NT와 많은 약점들을 공유하는데 독점적인 성질, 약점을 인정하는데서의 Microsoft의 좋지 않은 태도 그리고 Windows제품을 리용하는것과 관련한 비용 등의 문제들이다. NT와 류사하게 Windows 2000도 사용자친절성과 망에서의 일관성이라는 우점을 가진다.

Windows 2000은 NT와 구별되는 몇가지 우점을 가지고 있다. 첫째로는 봉사기를 재기동할 필요없이 구성변화를 할수 있는 능력이다. 둘째로는 봉사기의 안정성을 높인것인데 이것으로 하여 가동시간이 길어 지게 된다(또한 믿음성도 증가한다.).

많은 전문가들은 W2K가 NT에 비하여 얼마나 안전한가를 결정하는것은 아직 이르며 잠재적인 오유들과 취약성들을 폭로하는데는 아직 더 많은 시간이 필요하다고 믿고 있다. W2K의 일부 취약성들은 이미 발견되였고 수정되였다. 그것은 Telnet봉사였는데 여기서 해커는 관리적인 Telnet대화의 완전한 조종권을 가지고 전체 봉사기(잠재적으로 전체 망)를 손상시키고 위험에 빠지게 할수 있었다.

응용기초 방화벽

응용에 기초한 방화벽은 전용하드웨어 또는 쏘프트웨어에서 돌아 가며 보통 물리적으로는 전원과 망련결을 가지는 통으로 되여 있다. 여기에는 다음의 제품들이 포함된다.

- Cisco Pix
- Check Point VPN-1
- eSoft Interceptor
- Progressive Systems Phoenix Adaptive Firewall
- SonicWALL PRO
- Watch Guard LiveSecurity system 4.1

이러한 방화벽들에서는 제작자가 한 장치안에 하드웨어, 쏘프트웨어 그리고 조작체계까지 다 넣어서 제공한다. 이러한 장치들은 전적으로 봉사하는 IT전문가를 가지고 있지 않으며 기초적인 방화벽기능만을 필요로 하는 작은 기업들에서 많이 리용한다. 큰 기업들에서는 보다 비싸고 고급한것들을 리용하는데 이것들은 인터네트와 전자상업싸이트와 같은 큰 망들에서 발생하는 대량의 자료흐름을 처리하게 된다.

응용에 기초한 방화벽의 우점

이 종류의 방화벽의 가장 큰 리점은 짧은 구성시간이다. 많은 방화벽들은 망을 보호하도록 미리 구성되여 있다. 인터네트를 그 통의 한 포구에 련결하고 내부망을 다른 포구에 련결하면 장치는 즉시 망자료흐름을 려파하기 시작한다. 작은 기업들에서는 이 간단성으로부터 리득을 보는데 특히 또는 경험 있는 IT전문가를 가지고 있지 않을 때 유리하다. 만일 구성이 필요하다면 간단한 Web열람기 또는 전용의 관리도구프로그람에 의하여 관리가 진행된다.

성능도 이러한 형태의 방화벽의 우점으로 된다. 이 방화벽들은 프로그람가능한 하드웨어들을 리용하므로 조작체계와 하드웨어를 따로 가지는 방화벽들보다 높은 속도로 동작할수 있다.

이러한 전용설계방법은 방화벽의 가격을 낮출수 있는 가능성도 가지고 있다. 그것은 조작체계에 대한 구입 및 방화벽응용프로그람에 대한 추가적인 허가권에 대한 요구가 없기때문이다. 모든것은 제작자에 의하여 하나로 집적화된 통안에 들어 있다. 이 일체식방법(모든것이 제작자에 의하여 조종되고 설계되고 지원된다.)은 사실상 거기에 닿는 손들의 수를 최소화함으로써 보안을 강화할수 있다.

응용에 기초한 방화벽의 약점

한편 이러한 일체식방법은 제품의 유연성 또는 기초하드웨어의 갱신능력(봉사기에 기초한 방화벽에서 요구되는대로 더 많은 RAM을 설치하는것과 같은)에서 제한성이 있다. 또한 이 방법은 하나의 기관이 자기의 보안체계로 하여 하나의 제작자에게만 제한되게 된다.

응용에 기초한 방화벽은 또한 간단한 프로그람적실현에 비하여 비싼것으로 알려 져 있으며 기관이 요구하는 복잡성의 준위에 따라 전통적인 쏘프트웨어방화벽을 리용하는것이 더 좋을수도 있다.

방화벽의 기타 문제

어떤 형식의 방화벽을 선택하든지간에 특정의 방화벽제품을 사들이기전에 면밀히 분석해 보아야 할 몇가지 잠재적인 특징들이 있다. 이 특징들은 방화벽의 모든 형태들에서 공통적이므로 여기서 그것들을 두 부분으로 나누어 간단히 보기로 한다.

- 방화벽기능
  - 주소변환
  - 방화벽가입등록과 분석

- VPN
- 관리
    - 침입검출과 응답
    - 통합과 배비
    - 인증/접근조종/LOAP
    - 제3자의 도구들

이 절에서는 이 매개 특징들과 방화벽제품을 선택할 때 고려하여야 할 문제점들을 보기로 한다.

주소변환

주소변환은 기초적인 방화벽기능으로 간주된다. 이 기능을 포함하지 않는 방화벽제품은 믿지 말아야 한다. IP주소가 한 값으로부터 다른것으로 변환될 때 그것을 주소변환이라고 한다.

이 특징은 대부분의 방화벽제품들에서 실현되였으며 대표적으로 원격체계로 하여금 내부체계의 진짜IP주소를 알지 못하게 하려고 할 때 리용된다.

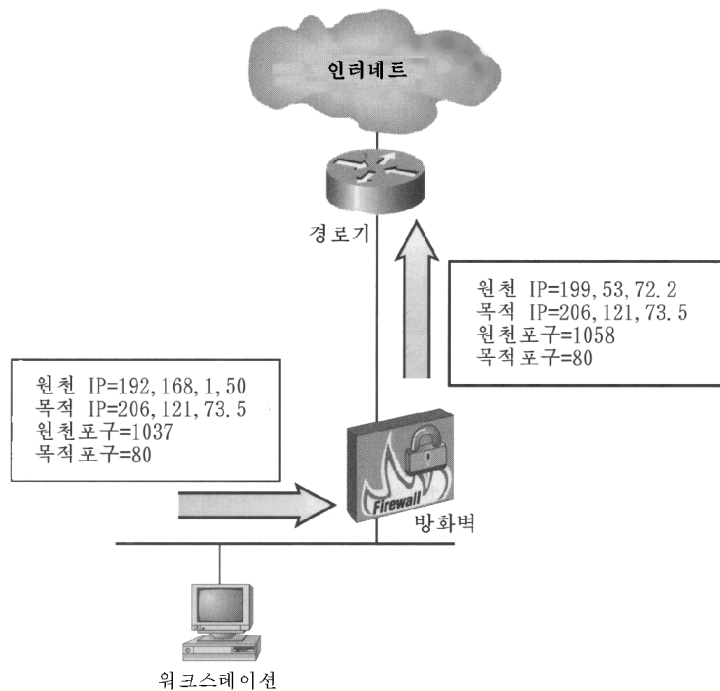



그림 5-12. 주소변환

그림 5-12는 이 구성의 대표적인 배비를 보여 준다.

내부워크스테이션은 외부Web싸이트에 접근하기를 원한다. 그것은 하나의 요청을 만들어 그 정보를 자기의 기정관문에 보내는데 이 경우에 이것은 방화벽이다. 탁상체계는 하나의 작은 문제를 가지고 있는데 그것은 그것이 위치하고 있는 부분망이 사설주소배당을 리용하는것이다.

사설주소배당이란 하나의 기관이 자기의 내부호스트들을 주소배당할 때 리용할수 있는 IP부분망대역의 리용이다. 이것은 이 대역이 인터네트에서 경로조종되도록 허용되지 않고 있기때문에 리용가능하다. 이것은 충돌한다는 걱정이 없이 이 주소들을 쓸수 있다는것을 의미하지만 또한 원격체계에 보낸 어떤 요청이 응답되려면 어느 경로를 취해야 하는가 하는것을 모른다는것을 의미한다.

이 대역들은 다음과 같다.

- 10.0.0.0 −10.255.255.255
- 172.16.0.0 −172.32.255.255
- 192.168.0.0 −192.168.255.255

포구번호에 모든것이 다 있다

방화벽은 어떻게 이 워크스테이션으로 돌아 오는 응답들과 다른 체계 또는 방화벽자체를 목적지로 하고 오는 자료흐름을 구별하는가? 만일 방화벽이 모든 탁상체계들의 주소를 변환하여 자기의 대면부의 주소와 맞추어 본다면 그것은 각이한 대화들사이의 차이를 어떻게 말할것인가?

그림 5-12의 두개의 파케트머리부를 자세히 보면 변화된 값들을 알수 있을것이다. 원천 IP주소와 함께 방화벽은 원천포구번호로 변화시켰다. 이 포구번호는 어느 응답이 어느 체계에로 가는가를 식별하는데 리용된다.

원천포구는 전송체계에 의하여 동적으로 배당되는 값이라는것을 기억하시오. 이것은 1023우의 어떤 값은 허용가능한것으로 간주된다는것을 의미한다. 방화벽은 이 값을 계산목적으로 쉽게 변경시킬수 있다. 원천포구번호를 체계들사이에서 여러 통신대화들을 구별하는데 리용하는것과 같은 방법으로 방화벽은 어느 응답이 우리의 내부체계들에 돌아 와야 하는가 하는것을 기억해 두기 위하여 이 원천포구번호를 리용할수 있다.

우리의 방화벽은 그 방법으로 IP머리부정보를 변경시켜 그것의 최종목적지에로 그 파케트를 전송한다. 돌아 올 때 우리의 방화벽은 그 자료를 내부체계에 전송하기 위하여 IP머리부를 다시 변경시켜야 할것이다. 응답파케트에서 변화되여야 하는것은 목적지IP주소와 봉사포구이다. 그것은 원격봉사기가 방화벽에 의하여 규정된 IP주소와 원천포구에 응답할것이기때문이다. 방화벽은 정보를 통과시키기전에 이 값들을 탁상워크스테이션에서 리용된것과 교체하여야 한다.

그러므로 우리의 워크스테이션은 원격봉사기에 도달할수 있으나 원격봉사기는 응답을 할수 없게 된다. 이것으로 하여 주소변환이 필요하게 되였다. 우리는 워크스테이션의

IP주소를 어떤 다른 합법적인 IP주소로 넘길수 있다. 그림 5-12의 경우에 우리는 탁상콤퓨터의 IP주소 192.168.1.50을 방화벽의 외부대면부에서 리용되는 합법적인 주소 199.53.72.2로 변환하였다.

주소변환을 배비하는데 세가지 방법이 있다.

- 숨겨 진 망주소변환(숨겨 진 NAT)
- 정적망주소변환(정적NAT)
- 포구주소변환(PAT)

매개 방법의 우점과 제한성을 고찰하기로 한다.

숨겨 진 NAT

숨겨 진 NAT는 정확히 그림 5-12에서 서술한것처럼 기능한다. 모든 내부IP호스트들은 하나의 IP주소뒤에 숨겨 진다. 이것은 방화벽 그자체의 IP주소일수 있고 어떤 다른 합법적인 번호일수도 있다. 숨겨 진 NAT는 리론적으로 수천개의 병행대화를 지원할수 있으므로 보충적인 지원을 요구한다면 여러개의 숨겨 진 주소들이 리용될수 있다.

숨겨 진 NAT의 가장 큰 제한성은 그것이 내부에로의 대화를 만들지 못하게 한다는것이다. 모든 체계는 하나의 주소뒤에 숨어 있으므로 방화벽은 원격대화요청이 어느 내부체계를 목적지로 할것인가를 결정할수 없다. 내부호스트에로의 넘기기가 없으므로 모든 내부로의 대화요청은 차단된다.

이 제한성은 그것이 보안대책을 강화할수 있다고 볼 때 사실상 하나의 중요한 특징이라고 간주할수 있다. 만일 보안방책에서 내부사용자는 자기의 내부탁상콤퓨터로부터 자기의 봉사기(Web, FTP 등)들을 돌리게 허용되여 있지 않다면 모든 탁상콤퓨터들에 대하여 숨겨 진 NAT를 리용하는것은 이 봉사들이 방화벽의 밖으로부터 직접 접근될수 없게 담보하는 빠른 방법으로 된다.

정적 NAT

정적NAT는 숨겨 진 NAT와 류사하게 기능하는데 다른것은 하나의 사설IP주소만이 매개 공적인 IP주소에 넘기기된다는것이다. 이것은 사설IP주소들을 리용하는 하나의 내부체계를 가지고 있지만 이 체계가 인터네트로부터 접근가능하게 하려고 할 때 유용하다. 하나의 내부호스트만이 매개 합법적인 IP주소와 련관되므로 방화벽은 자료흐름을 어디로 전송할것인가를 쉽게 결정할수 있다.

실례로 하나의 내부 Exchange봉사기를 가지고 있고 SMTP기능을 가능으로 함으로써 인터네트에서 우편을 교환할수 있게 하려고 하고 있다고 가정하자. Exchange봉사기는 IP주소 172.25.23.13을 가지고 있는데 이것은 사설주소공간으로 볼수 있다. 그러므로 호스트는 인터네트에 위치한 호스트들과 통신할수 없다.

다음과 같은 두가지 선택을 가진다.

- Exchange봉사기가 위치한 전체 부분망에 대하여 그 주소들을 사설주소로부터 합법적인 주소로 변화시킬수 있다.
- 방화벽에서 정적NAT를 수행할수 있다.

명백히 두번째 선택이 더 실행하기 쉽다. 그것은 내부체계들로 하여금 자기에게 배당된 사설주소를 리용하여 Exchange봉사기와 계속 통신할수 있게 하며 모든 인터네트통신들을 하나의 가상적인 합법적IP주소로 변환한다.

정적NAT는 또한 숨겨 진 NAT에서는 차단하는 봉사들에 대해서도 유용하다. 실례로 DNS봉사기들사이의 어떤 통신은 원천 및 목적지포구가 둘다 포구53에 설정될것을 요구한다. 만일 숨겨 진 NAT를 리용한다면 방화벽은 원천포구를 어떤 우연적인 웃포구번호로 바꿈으로써 통신대화를 차단하게 될것이다. 정적 NAT를 리용하면 포구번호는 변화되지 않아도 되고 통신대화가 정상으로 수행될수 있다.

일러두기

대부분의 NAT장치들은 정적 및 숨겨 진 NAT를 동시에 리용할수 있게 한다. 이것은 정적NAT가 필요한 체계에서는 그것을 쓰고 나머지에서는 숨겨 진 NAT를 쓸수 있게 한다.

포구주소변환(PAT)

포구주소변환은 대부분의 대리자방화벽제품들에서 리용된다. PAT가 리용될 때 모든 밖으로의 통신은 숨겨 진 NAT와 류사한 방법으로 방화벽에 의하여 리용되는 외부IP주소로 변환된다. 숨겨 진 NAT와 달리 방화벽의 외부주소가 리용되여야 한다. 이것은 어떤 다른 합법적인 값으로 설정될수 없다.

내부에로의 자료흐름을 취급하는 방법은 제품에 따라 다르다. 어떤 실현에서 포구들은 특정의 체계에로 넘기기한다. 실례로 방화벽의 외부대면부에로 향하는 모든 SMTP통신은(이것은 목적지포구번호 25를 가진다.) 자동적으로 특정의 내부체계에로 전송한다. 작은 환경에서 이 제한은 거의 문제로 되지 않는다. 많은 체계들이 같은 형태의 봉사기(다중우편 또는 FTP봉사기와 같은)를 돌리고 있는 큰 환경에서 이것은 큰 문제로 된다.

이 문제를 극복하기 위하여 어떤 봉사기들은 여러개의 내부봉사들을 지원하기 위하여 자료내용을 분석할수 있다. 실례로 어떤 대리자는 user @ eng. bofh. org로 주소지정된 모든 들어 오는 SMTP우편들을 하나의 내부우편체계에로 전송하고 user @ hr. bofh. org로 주소지정된 우편들은 다른것에로 전송한다.

만일 같은 봉사를 돌리는 여러개의 내부봉사기를 가지고 있다면 방화벽이 그것들을 구별할수 있는가를 확인해 보아야 한다. 이러한 제한에 의하여 곤난해 지고 봉사기들을 방화벽의 밖에 배치하지 않으면 안되게 되였던 실례들을 많이 들수 있다.

방화벽가입등록과 분석

방화벽의 기본기능은 망경계선에서의 자료흐름을 조종하는것이고 다음으로는 자기가 만나는 모든 자료흐름을 등록하고 분석하는것이다. 등록은 누가 망경계를 통과하였고 또 누가 통과하려고 시도하였으나 실패하였는가를 문서로 만드는것으로서 매우 중요하다. 분석은 어느 사건들이 실례로 방어선을 통과하려는 시도인가 그리고 어느것이 앞으로의 공격을 위한 준비로서 《담장》을 열어 보는 연구인가 하는것이 등록파일만 보는것으로

는 쉽게 할수 없으므로 중요하다.

무엇이 좋은 방화벽등록을 정의하는가? 명백히 이것은 사람에 따라 다르다. 그러나 고려하여야 할 많은 특징들이 있다.

- 등록파일은 모든 항목들을 명백하고 읽기 쉬운 형식으로 제출하여야 한다.
- 등록자료를 분석도구에로 보내는것이 보다 효과적일수도 있지만 하나의 표의 모든 항목들을 보고 자료흐름패턴을 더 잘 식별할수 있어야 한다.
- 등록파일은 어느 자료흐름이 차단되였고 어느 자료흐름이 통과되였는가를 명백히 식별하여야 한다.
- 분석도구프로그람으로 할수도 있겠지만 려과와 정렬을 리용하여 등록파일을 처리하여 특정형식의 자료흐름에 집중할수 있어야 한다.
- 등록파일은 정해 진 크기제한에 따라 항목들을 겹쳐 쓰거나 빠뜨리지 말아야 한다.
- 등록파일을 원격위치로부터 안전하게 볼수 있어야 한다.
- 등록프로그람은 어떤 방법으로 이 등록파일을 ASCII와 같은 적어도 한가지 공통적인 형식으로 출구할수 있어야 한다. 이렇게 하면 그 자료를 다시 기록도구, 표처리프로그람 또는 자료기지프로그람으로 처리할수 있다.

이 특징들이 모두가 다 중요한것은 아니다. 공격자가 첫 시도에서 접근을 얻는것은 매우 드물다. 만일 규칙적으로 등록파일을 세밀히 분석한다면 공격이 발생하기전에 그것을 좌절시킬수도 있다. 좋은 등록도구가 매우 중요하다.

fw.log - FireWall-1 Log Viewer

No	Date	Time	Inter.	Action	Service	Source	Destination	Prot..	Rule	S_Port
1	26Aug97	20:50:19	DC21X41	drop	ftp-data	Herne	SKYLAR	tcp	2	1237
2	26Aug97	20:50:19	DC21X41	accept	ftp	Herne	SKYLAR	tcp		
3	26Aug97	20:50:20	DC21X41	drop	22	Herne	SKYLAR	tcp	2	1239
4	26Aug97	20:50:20	DC21X41	accept	telnet	Herne	SKYLAR	tcp		
5	26Aug97	20:50:21	DC21X41	drop	24	Herne	SKYLAR	tcp	2	1241
6	26Aug97	20:50:21	DC21X41	accept	smtp	Herne	SKYLAR	tcp		
7	26Aug97	20:50:22	DC21X41	drop	26	Herne	SKYLAR	tcp	2	1243
8	26Aug97	20:50:22	DC21X41	drop	27	Herne	SKYLAR	tcp	2	1244
9	26Aug97	20:50:23	DC21X41	drop	28	Herne	SKYLAR	tcp	2	1245
10	26Aug97	20:50:24	DC21X41	drop	29	Herne	SKYLAR	tcp	2	1246
11	26Aug97	20:50:24	DC21X41	drop	30	Herne	SKYLAR	tcp	2	1247
12	26Aug97	20:50:25	DC21X41	drop	31	Herne	SKYLAR	tcp	2	1248
13	26Aug97	20:50:25	DC21X41	drop	32	Herne	SKYLAR	tcp	2	1249
14	26Aug97	20:50:26	DC21X41	drop	33	Herne	SKYLAR	tcp	2	1250
15	26Aug97	20:50:26	DC21X41	drop	34	Herne	SKYLAR	tcp	2	1251
16	26Aug97	20:50:27	DC21X41	drop	35	Herne	SKYLAR	tcp	2	1252

For Help, press F1 | logview.fw | 127.0.0.1 | NUM

그림 5-13. 방화벽-1의 등록파일보기

실례로 그림 5-13에서 보여 준 등록파일보기를 고찰하자. 이것은 방화벽-1의 등록파일보기인데 그것은 우리가 목록화한 규준들을 집행하는 매우 좋은 일을 하고 있다. 이 등록파일은 읽기 쉽고 따라 가기 쉬우며 안전한 대화를 통하여 다른 워크스테이션으로부터 원격으로 볼수도 있다.

Select menu선택에 의하여 여러가지 려과 및 정렬선택들을 얻을수 있다.

그림 5-13의 매 파케트항목에 기록된 봉사들을 따져 보자. 이상한것은 없는가? 우리의 원천체계 Herne가 매개 TCP봉사포구들에서 Skylar에게 련결하려고 시도하고 있는것으로 나타난다. 이 화면은 봉사포구 20(FTP-자료)에서 시작하여 한번에 한 포구씩 포구 35까지 계속하고 있다. 이것은 Herne이 어떤 봉사가 제공되고 있는가를 알기 위하여 Skylar에 대하여 하나의 포구스캐너를 돌리고 있다는것을 가리킨다.

이에 대조되는것으로서 Secure Computing의 BorderWare방화벽에서 리용된것과 같은 등록파일보기가 있다. 이 방화벽은 6개이상의 등록파일을 가지고 있다. 이것은 특정한 봉사를 기록하는것은 좀 쉽지만 특정의 호스트를 기록하는것은 보다 어렵다. 이 정보를 결합하기 위하여서는 제3자의 프로그람을 리용하여야 하며 무엇이 진행되고 있는가를 명백히 보아야 한다. 또한 그림 5-13의 등록파일들은 간단한 차림표선택에 의하여 출구되거나 보관될수 있지만 BorderWare는 FTP관리를 가능으로 하고 수동으로 그 파일을 국부콤퓨터에 전송할것을 요구한다.

일러두기

방화벽제품을 선택할 때 등록파일대면부가 유연하여야 한다는것을 명심하여야 한다. 방화벽의 ACL은 보통은 설정되여 있고 매우 적은 변화를 요구하므로 등록파일을 보고 자료흐름을 분석하는데 매우 적은 시간을 소비할것을 계획하여야 한다.

가상사설망

가상사설망(VPN)은 고성능의 방화벽을 구성할수 있게 하는 특징으로 간주되고 있다. VPN은 인증되고 암호화된 접근이 공공의 인터네트를 통하여 인트라네트에로 실현될수 있게 한다. 이것은 비싼 점대점통신대신에 LAN 또는 이동사용자가 값 눅은 ISP를 리용하여 자기의 내부기관의 자원과 통신할수 있다는것을 의미한다.

그러나 그저 기초적인 VPN봉사만을 제공하는것으로는 충분하지 않다. 자기의 방화벽이 VPN을 위하여 어떤 구성, 관리, 암호화선택을 제공할것인가를 결정하여야 한다. 어떤 경우에는 방화벽에 통합된 전용VPN이 가장 좋은 결과를 제공할수 있다.

침입검출과 응답

공격이 진행되는것을 관리자에게 알리기 위한 방화벽의 능력도 구입 및 배비를 결정하는데서 고려되여야 한다. 2000년 2월에 발생한 높은 급의 DoS(봉사거부)공격의 경우에 방화벽체계가 IT담당자에게 비정상적인 망동작에 대하여 인차 알림으로써 여러개의

싸이트들은 한시간내에 정상기능으로 돌아 오게 되였다.

미래의 방화벽체계는 공격이 있는 경우에 전체 망이 응답하고 자신을 재구성하도록 하는 일정한 협동동작을 약속하고 있다. 전문가들은 이러한 수준의 혁신적인 감시와 응답에 관한 기술이 가능하다고 보고 있으나 도전은 여전히 제기되고 있다. 실제로 효과적이기 위하여서는 서로 다른(지어 경쟁하는) 기관이나 기업이라고 하여도 모든 영향 받는 집단들이 협동동작하고 통신하여야 한다.

공격자는 정체를 유지하기가 더 어려울것이며 공격의 효과는 매우 빨리 중화될것이다.

침입과 비루스(2000년 3월에 있은 《I Love You》와 같은) 등에 대하여 감시하고 기록하는 공식적인 또는 비공식적인 집단들이 이미 존재한다. 그러나 기록하는 방식들은 흔히는 수동적이며 《눈에 의한》방법이 요구되고 있다. 리상적으로 기록은 자동적이고 규격화되여야 하며 모든 자동적인 또는 혁신적인 방어작용들을 가능하게 하는 충분한 정보를 가지는 지능적인 체계가 있어야 한다.

통합과 접근조종

방화벽은 다른 망체계 및 봉사들과 더욱더 통합되고 있다. 이렇게 하면 방화벽이 현존망의 기반구조를 중복시키지 않으므로 관리를 간단하게 하고 복잡성을 줄이며 TCO(Total Cost of Ownership: 소유총비용)을 증가시키게 된다.

통합의 실례로는 여분의 사용자구좌정보를 없애고 선택가능한 인증기구를 도입하는 등록부 및 인증을 들수 있다. 이러한 봉사를 제공하는 두가지 공업규격이 있는데 LDAP(가벼운 등록부접근규약)과 RADIUS(원격인증전화접속사용자봉사)이다.

가벼운 등록부접근규약(LDAP)

LDAP는 두 등록부봉사사이에 또는 하나의 등록부봉사와 의뢰기사이에 통로를 만든다. 방화벽에 있어서 이것은 사용자 및 집단의 구좌를 여분으로 만들 대신에 체계가 제3자의 등록부봉사에 보관되여 있는 구좌들과 등록정보들을 리용하여 접근을 결정할수 있다는것을 의미한다. 이것은 중복되는 사용자 및 집단의 구좌를 만들고 관리하는 관리부담을 감소시키는 직접적인 리득을 가져다 주며 또한 보안체계의 가장 큰 적인 복잡성을 감소시킨다.

등록부봉사의 실례로는 Microsoft의 AD(Active Directory), 노벨의 NDS (NetWare Directory Service), iPlanet의 등록부봉사기 등을 들수 있다.

원격인증전화접속사용자봉사(RADIUS)

RADIUS는 인증을 위하여 하나의 확장가능하고 독립적인 플래트홈을 제공한다. 이것은 변경가능한 인증기구(스마트카드 또는 생물측정장치와 같은)를 제공할뿐아니라 RADIUS봉사기들은 방화벽으로부터(또는 LDAP 에 따르는 등록부봉사들) 실제적인 인증작업부담을 덜어 준다.

인증만을 위한 기반구조를 제공함으로써 RADIUS는 인증과정(그리고 결과적으로는

접근과정)을 간단화하고 강화한다.

제3자의 도구

많은 현대 망들은 많은 서로 다른 제작자들의 여러가지 기술의 《프랑켄슈타인》이다. 이것은 기술의 최량적인 집합일수 있으나 관리하기에는 하나의 악몽과 같을수 있다(역자: 프랑켄슈타인: Frankenstein: 환상소설의 주인공인 과학자의 이름. 자기가 만든것에 의하여 파멸되는 사람).

다행히도 모든 망장치들과 응용프로그람들을 중앙집권적으로 감시하고 관리하도록 설계된 새로운 기술들이 나타나고 있다. 한가지 훌륭한것은 HP의 OpenView인데 이것은 다음의 분야들에서의 관리를 제공한다.

- 응용프로그람들
- 리용성(Availability)
- 망
- 성능
- 봉사
- 체계
- 저장 및 자료

방화벽이 제3자의 관리도구를 가지고 일할수 있는 능력은 어느 제품을 선택하는가 하는데서 결정적인 인자로 될수 있다.

그러나 관리는 제3자의 제품을 찾을수 있는 유일한 분야는 아니다.

Check Point의 VPN-1은 다른 제작자들이 자기들의 특징을 URL려과, 반비루스주사 그리고 전자우편스팸보호까지 포함하도록 확장할수 있게 한다. 이러한 추가적인 리점들로 하여 이러한 제품들의 가격은 보통 비싸다.

자신이 결심하라

매개 선택에 대하여 몇가지 강한 론점들이 존재한다. 자기의 환경에 맞는 선택을 하기 위하여서는 이 모든 론점들을 조사해 보고 어느것이 특정의 환경에 더 잘 적용될수 있겠는가를 결정하여야 한다.

표 5-6은 대표적인 방화벽제품들을 가격, 특징 그리고 플래트홈별로 분석한다.

방화벽의 배비

이제 하나의 방화벽제품을 선택하였다고 하자. 이제 큰 문제는 그것을 망환경에 어떻게 설치할것인가 하는것이다. 이 문제에는 여러가지 방법이 있지만 가장 일반적인 배비는 그림 5-14에 보여 준것과 같다.

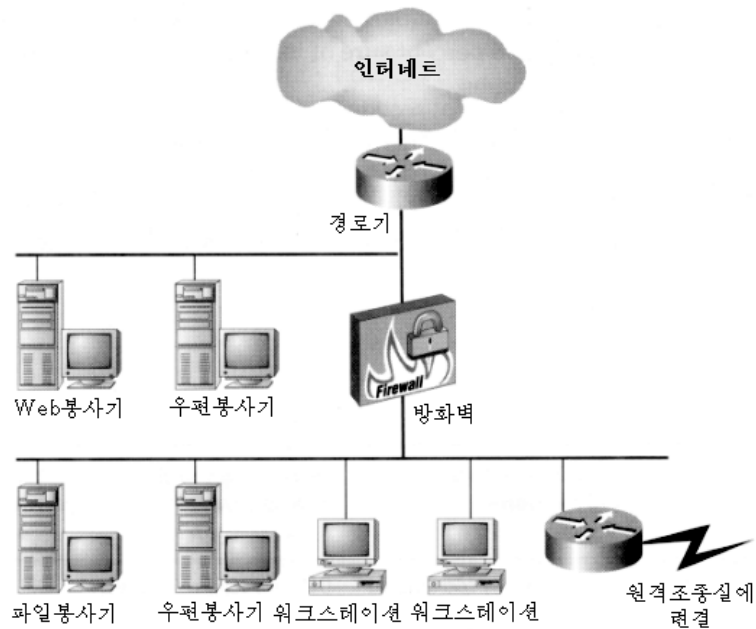



그림 5-14. 방화벽을 어디에 놓을것인가?

표 5-6 대표적인 방화벽제품들의 비교

이름	봉사(정적/동적/상태/대리자)	조작체계 (또는 응용)	주소 변환	방화벽등록 및 분석
Check Point VPN-1 Appliance 330	모두	응용	있음	포구, 봉사, 규약 및 시간에 의한 감시
Cisco Secure PIX FireWall Model 515-R-BUN	모두	응용	있음	덧붙임(Cisco Secure Policy Manager)
ESoft Interceptor	모두	BSD Unix	있음	지원 없음
Progressive System Phoenix Adaptive FireWall	모두	응용	있음	자료만 출구
SonicWALL PRO	모두	응용	있음	제한, 분석 없음
Watch Guard LiveSecurity System4.11	모두	응용 (Linux OS), Windows 응용 프로그람에 의하여 설치, 관리	있음	실시간등록, 분석

표계속

이름	VPN	침입검출 및 응답	통합과 접근조종	다른 봉사들 (제3자의 도구포함)
Check Point VPN-1 Appliance 330	있음 (Ipsec)	중심자리표	DES, 3DES, IKE, IPSec, RADIUS, Secure ID, S/Key, TACACS, TACACS +, LDAP	URL려과, 반비루스주사, 전자우편스팸보호
Cisco Secure PIX FireWall Model 515-R-BUR	IPSec, PPTP	Cisco Secure Policy Manager	RADIUS, TACACS+	반비루스, URL막기
ESoft Interceptor	ICPSec (선택), PPTP (표준)	Pager, e-mail, SNMP	CryptoCard, RADIUS, SecureID Card, S/Key	SiteBlocker, AOL, filer rule, NNTP packet screening remote shell, Rlogin RTSP, security 스캐너 SNMP, Spamfilter VDOlive, Xwindows체계
Progressive System Phoenix Adaptive FireWall	독점 (앞으로는 Ipsec)	반공격표구주사 (경보능력 없음)	Entrust, RADIUS, SecurID, Security Dynamics ACE server, LDAP	없음
SonicWALL PRO	IPSec, PPTP	전자우편	56bit DES, 3DES	AutoupdateCookies, Java, NNTP, Proxy Blocking
WatchGuard LiveSecurity System4.11	PPTP	전자우편 Pager	PcryptoCard, Internal ACL Microsoft Windows NT, RADIUS, SecurID	NetMeeting, (하드웨어, based on Linux 2.0 핵심부), SNMP

이 설계에서 모든 내부체계는 인터네트에 기초한 공격으로부터 보호된다. WAN련결을 통하여 기관에 련결된 원격싸이트들도 보호된다. 인터네트로부터 접근가능한 모든 체계들(Web봉사기나 우편중계기와 같은)은 자기들의 부분망으로부터 격리된다. 이 부분망을 DMZ 또는 비무장지대라고 부른다. 그것은 이 구역이 공격에 안전할수 있지만 이 체계에로의 들어 가는 련결이 허용되고 있으므로 이 안전성을 100% 담보할수는 없기때문이다.

DMZ를 리용하면 공격으로부터의 보충적인 보호를 제공한다. 어떤 들어 가는 봉사들은 이 호스트들에게 열려 져 있으므로 공격자는 이 체계들에 대한 높은 급의 접근권을 얻을수 있다. 만일 이것이 발생한다면 보충적인 내부체계들이 손상될 가능성은 더 적게 된다. 그것은 이 체계들이 망의 나머지 부분들로부터 격리되여 있기때문이다.

다른 형식의 원격접근을 조종하기 위하여 방화벽에 추가적인 망기판이 보충될수 있다. 실례로 회사가 자기의 공식적인 성원이 아닌 기업상대와 WAN련결을 가지고 있다면 방화벽에 추가적인 NIC기판을 넣음으로써 또 하나의 부분망을 만들수 있다. 그러면 이 원격기업상대에 련결하는 모든 경로기들은 이 부분망에 배치되게 된다. 방화벽은 이 싸이트들과 내부 망사이에서 자료흐름을 조종할수 있게 된다.

추가적으로 보안을 더 강화하기 위하여 자기의 경로기의 정적파케트려과기능을 리용할수 있다. 이것은 망방어선에 여러층의 보호벽을 쌓는것으로 된다. 만일 보안장치들중의 하나에서 한가지 약점이 발견된다면 두번째 장치가 그 약점을 메꿀수 있게 된다.

이 기초적인 설계의 많은 변종들이 존재한다. 실례로 보안을 더욱 강화하기 위하여 그림 5-14에 보여 준 구성에다 추가적인 방화벽형태를 보충할수 있다. 실례로 그림에서의 방화벽이 동적파케트려과기라면 자기의 인터네트련결을 더 안전하게 하기 위하여 그 뒤에 대리자방화벽을 설치할수 있다.

일러두기

모든 통신대화가 방화벽을 통하여 지나가도록 하기 위하여 인터네트와 보호하려고 하는 자산사이에 방화벽을 설치하는것이 항상 좋은 생각으로 되지는 않는다는것을 기억하시오.

요 약

여기서는 방화벽과 그것이 어떻게 동작하는가에 대하여 결론 지으려 한다. 방화벽의 기초적인 형태와 모든 방화벽들이 제공하는 봉사들을 보면 다음과 같다.

- 정적/동적/상태/대리자려과
- VPN능력
- 감시, 등록 및 분석
- 그밖의 봉사들과 제3자의 제품통합

이제는 자기의 보안 및 기업요구에 맞는 방화벽을 선택할수 있는 지식을 갖추게 되였다.

다음의 두 장들에서는 몇가지 특정의 방화벽제품들을 어떻게 설치하고 구성하겠는가 하는 실례들을 고찰할것이다.

제6장. Cisco경로기의 보안특징

지금까지는 방화벽리론과 어떻게 그 장치들이 자료흐름을 려파하는가를 고찰하였다. 이 장에서는 망방어선을 안전하게 하기 위하여 Cisco경로기를 어떻게 구성할것인가를 보기로 한다.

Cisco는 인터네트련결을 제공하는데서 기본적인 제품제공자로 되였으며 많은 사람들이 자기의 인터네트봉사제공자에 련결하기 위하여 Cisco경로기를 사용하고 있다. 경로기는 전문으로 WAN련결을 위하여 요구되는 설비이므로 Cisco보안특징들을 어떻게 구성할것인가를 아는것은 기업상대들사이의 자료흐름을 조종하는데서 쓸모가 있을것이다.

Cisco경로기

Cisco는 론쟁할 여지없이 하드웨어경로기의 첫째가는 공급자이다. 그것은 다양한 생산선을 가지고 있는데 이것은 그가 거의 모든 구성요구에 맞는 경로기를 가지고 있다는것을 의미한다. ISP에 련결하기 위하여 상사식전화접속, ISDN, 임대선, 프레임중계, T1 또는 지어 T3회로를 쓴다고 하여도 Cisco는 그 요구에 맞을수 있는 많은 제품을 가지고 있다.

Cisco경로기계렬의 한가지 특이한 능력은 IOS 11.3과 같은 재귀적려파가 제공된다는것이다. 재귀적려파는 Cisco경로기가 련결대화상태를 유지하게 한다. 이것은 대부분의 경로기들은 정적려파만을 지원하지만 IOS 11.3 또는 그이상급을 리용하는 Cisco경로기는 동적파케트려파를 수행할수 있다는것을 의미한다. 이것은 완전성능의 방화벽을 필요로 하지 않는 작은 기관이나 또는 완전성능의 방화벽은 너무 비싸다고 여기는 환경에서 쓰기에 매우 리익이 된다(기업상대와의 WAN련결과 같은것). 이 특징모임도 또한 추가적인 방화벽대책과 결합되여 방어선을 더욱 강화할수 있다. 보다 새로운 IOS 12.1을 돌리는 Cisco경로기들은 또한 련결시간과 문맥에 기초하여 려파할수 있으므로 보안장치로써의 쓸모가 더욱 커지고 있다.

인터네트련결을 위하여 경로기를 선택할 때 대부분의 기관들은 전통적으로 Cisco 2500 계렬의 경로기를 선택하였다. 그러나 2500계렬의 경로기들은 확장가능하지 못하기때문에 회사들은 보다 새로운 실현으로써 2600계렬을 구입하기 시작하였다. 그것은 모듈형식이고 확장가능하며 다른 Cisco경로기계렬들과 호환가능한 대면부를 가진다.

또한 기업들은 자기들의 망에 고속이써네트(100Mbps), 기가비트이써네트(1000Mbps), VLAN(가상국부망), VPN, 수자식전화 그리고 다매체흐름 등과 같은 보다 새로운 기술들을 받아 들이기 시작하였다. 이 요구는 하나의 제작자에게 있어서도 경로기제품들의 종류를 크게 증가시켰다.

2500 및 2600계렬의 널리 쓰이는 모형들에 대한 요약를 표 6-1에 주었다. 이전의 Cisco모형들은 주로 이써네트토막에 대하여 Attachment Unit Interface(AUI)련결을 리용하였으므로 이때에는 송수신기까지도 구입하여야 하였다.

주 의

송수신기는 AUI련결에서 리용된 DB15다리접속과 꼬임쌍선환경에서 리용된 RJ45암접속사이를 변화해 준다.

표 6—1 Cisco 2500과 2600계렬의 대표적인 모형들

모형번호	가지고 있는 포구	속 도
2503	1이써네트, 1BRI, 2직렬	128K ISDN, 10Mbps
2520	1이써네트(AUI), 1BRI, 1이써네트(RJ45), 1직렬	128K ISDN, 10Mbps
2610	1이써네트(RJ45), 1망모듈 확장홈, 2WAN대면부카트	포구에 따라 다름 (최대 100Mbps)
2611	2이써네트(RJ45), 1망모듈 확장홈, 2WAN대면부기판, 1AIM확장홈	포구에 따라 다름 (최대 100Mbps)

어디서 시작할것인가

Cisco경로기는 매우 유연성 있는 장치이다. 구성가능한 선택기능의 수는 솔직히 말하여 거대한 수에 달한다. 실례로 IOS 12.1(최근의 기본 OS발표)에 대한 직결《Cisco IOS쏘프트웨어지령요약집》은 수백페지에 달한다. 이것은 완전히 구체적인 지도서가 아니라 《요약집》인데도 주머니에 넣을수 있는 그런 작은것은 아니다.

Cisco경로기를 어떻게 구성할것인가 하는 완전한 서술은 이 책의 범위를 벗어 난다. 여기서는 간단히 이 장치를 리용하여 보안방책을 어떻게 실현할것인가 하는데 집중하기로 한다. 그러므로 우리는 다음의 내용들을 가정하겠다.

- IOS 12.0 또는 그이상급이 경로기에 적재되였다.
- 경로기에는 전원이 련결되였고 LAN과 WAN에 물리적으로 련결되였다.
- 두 대면부는 유효한 IP주소와 부분망마스크를 가지고 있다.
- 자기의 ISP에 위치한 WAN의 다른 끝에서 그 경로기에 Ping지령을 보낼수 있다.
- 독자는 Cisco지령대면부에 대하여 상당히 알고 있다.

이 요구들이 만족되면 자기의 방어선차단을 시작하기에 준비된것으로 된다.

기초적인 보안관련문제

방어선을 안전하게 하는데서 출발점은 경로기자체가 손상되지 않도록 담보하는것이다. 만일 공격자가 그 구성을 변경시킬수 있다면 경계선을 통과하는 자료흐름을 조종하는데서 경로기는 잘 리용되지 않을것이다. Cisco경로기는 여러가지 접근준위를 제공한다.

- 사용자EXEC방식
- 특권EXEC방식

사용자EXEC방식

사용자EXEC방식은 Cisco경로기에 련결할 때 사용하게 되는 첫 조작방식이다. 만일 직접조종탁대화를 돌리고 있다면 자동적으로 사용자EXEC방식에 있는것으로 된다. 만일 telnet대화를 통하여 경로기에 련결하고 있다면 먼저 말단통과암호를 입력해야 한다.

주 의

Cisco경로기는 말단통과암호가 설정되지 않았다면 모든 telnet대화시도를 거부할것이다.

Cisco경로기는 현재 어느 조작방식을 리용하고 있는가에 따라 말단입력차림표방식을 변화시킨다. 이 입력차림표는 항상 경로기의 이름으로 시작하고 사용자가 어디에 있는가를 알도록 하는 어떤 특수한 순서로 끝난다. 표 6-2는 일반적인 입력차림표들의 일부들을 보여 준다.

표 6-2　　　Cisco지령입력차림표

입력차림표	설 명
router>	사용자EXEC방식
router#	특권방식
router(config)#	전체구성방식
router(config-if)#	대면부구성방식

다른 입력차림표들의 의미에 대하여서는 지금은 걱정하지 않아도 된다. 다음절에서 그것들을 고찰할것이다.

사용자EXEC방식에서는 사용자가 련결을 검사하고 통계를 볼수 있지만 그 장치에 어떤 형태의 구성변화를 줄수는 없다. 이것은 말단통과암호가 손상되거나 또는 공격자가 그 장치에 물리적으로 접근할수 있을 때 공격자에 의하여 초래될수 있는 손실의 크기를 감소시킬수 있게 한다.

특권방식

사용자는 특권방식에 들어 가기전에 먼저 사용자EXEC방식에 들어 가야 한다. 이것은 공격자가 경로기에 완전접근을 얻으려면 두개의 통과암호를 깨야 한다는것을 의미한다. 특권방식은 기정에 의하여 큰 kahuna이다. 이 접근준위에서 사용자는 구성파라메터들을 자유롭게 변화시키거나 지울수 있다.

다음의 지령을 입력함으로써 특권방식에 들어 간다.

enable
password：privilege_password

특권적인 접근권을 얻기 위하여 지령 enable을 리용하므로 이 방식은 때로 enable방식이라고 부른다. 이전에는 통과암호를 변화시키기 위하여 다음과 같은 지령을 사용하였다.

enable password new_password

그러나 Cisco는 지금 보다 강한 암호화알고리듬을 리용하는 다음의 지령을 사용할것을 권고한다.

enable secret new_password

사실상 16개까지의(0~15) 특권준위접근을 규정할수 있는데 매개는 자기의 일의적인 통과암호를 가진다. 이 경우에 사용자가 특권방식을 접근할 때 입력하는 통과암호는 사용자가 어느 준위의 특권접근을 받고 있는가를 결정한다. 이것은 관리자가 어떤 특권준위지령에 접근한다면 유용할수 있지만 모두 그런것은 아니다. 특정의 특권준위에 대하여 통과암호를 설정하려면 다음의 지령을 입력한다.

enable secret level new_password

여기서 lebel은 0부터 15사이의 어떤 값으로 교체된다. 이 값이 작을수록 특권준위접근의 준위가 더 낮다.

모든 리용되지 않는 봉사들을 불가능으로 하기

어떤 망가능장치에 대한 한가지 일반적인 보안방법은 리용되지 않는 모든 봉사들을 불가능으로 하는것이다. 리용되지 않을 때 불가능으로 되여야 하는 봉사들의 실례로는 다음의것들을 들수 있다.

- SNMP
- NTP(망시간규약)
- CDP(Cisco발견규약)

주 의

NTP와 CDP는 기정으로 가능하게 된다. CDP를 불가능으로 하기 위해서는 no cdp run 지령을 사용한다. NTP에 대하여서는 NTP를 리용하지 않는 매 대면부에서 ntp disable지령을 사용한다.

가입등록화면을 변경시키기

가입등록화면을 변경시켜 선택적인 통보문이 현시되게 하는것이 한가지 좋은 생각이다. 공격자가 경로기에 접근하려고 할 때 그에게 《Welcome》이라는 통보문이 나타나도록 하는것이 최근의 류행이다. 그 통보문은 망하드웨어에 대한 권한 없는 접근에 대한

기관의 태도를 반영하여야 한다. 다음과 같은 명령으로 화면의 제목을 변경시킨다.

```
banner login # message #
```

여기서 #는 ASCII범위의 문자이다. 이 문자는 통보문안에서 리용할수 없으며 그 명령이 어디서 통보문이 끝나는가를 알도록 하기 위하여 리용된다. 통보문을 여러행으로 만들수 있다. 특권방식에서 이 명령을 리용하여야 한다.

이 명령의 한가지 실례는 다음과 같다.

```
banner login # Unauthorized access prohibited #
```

말단통과암호를 변화시키기

12.1에서 돌아 가는 Cisco경로기는 여러개의 병행적인 telnet대화를 지원할수 있다. 이 통과암호들을 규칙적으로 변화시키는것은 그 장치가 손상 당하지 않도록 담보하기 위한 좋은 생각이다. 이러한 련결들중 하나(먼저 기호 'O')에 대한 통과암호를 변경시키기 위하여서는 먼저 특권방식에 들어 가서 다음의 명령을 입력하여야 한다.

```
line vty 0
login
password 2SeCret4U
```

일러두기

Cisco통과암호들은 소문자, 대문자들을 구별하므로 통과암호를 알아 맞추기 어렵게 하려면 소문자, 대문자를 결합하는것이 좋다.

원격으로 접속할 때 어느 vty를 리용할지 선택할수 없으므로 Cisco는 모든 vty통과암호들을 같은 문자렬에 설정할것을 권고한다.

보다 강한 통과암호인증의 리용

지난 시기에 Cisco통과암호체계의 약점은 계산능력이 없는것이였다. 매 관리자는 같은 통과암호를 리용하고 있었으므로 누가 어떤 변화를 만들었는가를 알수 있는 조사결과가 없었다. IOS 12.0에서부터 시작하여 Cisco는 통과암호체계에서의 약점들을 보강하기 위하여 AAA(인증, 권한, 회계)라고 부르는 새로운 보안체계를 받아 들이였다.

인증 이것은 사용자를 식별하는 방법으로서 가입등록시 통과암호를 요구하는것, 물음에 응답하는것 그리고 암호화 등 여러가지를 통해서 할수 있다.

권한 이것은 접근을 조종하는 방법인데 1회용 또는 봉사에 기초한 권한, 사용자당 구좌, 사용자집단 그리고 규약에 기초한 접근조종(IP, IPX, ARA 및 telnet) 등이 있다.

회계 이것은 정보를 모으는 방법인데 망활동을 표로 만들고 조사하며 보고하는데 리용된다. 정보의 형식들로는 사용자신분, 시작 및 끝시간, 리용된 지령(FTP get와 같은) 파케트 또는 byte수 등이다. 회계를 통하여 사용자는 그들이 접근한 자원과 련관되게 된다.

Cisco는 AAA와 함께 RADIUS, TACACS+(말단접근조종자 접근조종체계) 그리고 Kerberos를 포함하여 공업규격화기술들을 실현할것을 선택하였다. AAA밖에서의 인증구성은 이 규격화들과 함께 동작할수 없다. 아래에서는 Cisco가 AAA에서 이것들을 어떻게 실현하는가를 보여 준다.

RADIUS 경로기들은 인증정보를 RADIUS봉사기에 전송하는 RADIUS의뢰기들이다.

TACACS+ UNIX 또는 NT기계에서 돌아가는 봉사에 의하여 자료기지가 유지된다. 경로기들은 TACACS+ 봉사에로의 요청을 통과시킨다.

Kerberos Kerberos는 사용자와 그들이 리용하는 망봉사들이 누구이며 무엇인가를 확인하는데 리용된다. 경로기는 권한 받은 사용자에게 배당된 Kerberos표를 분석하여 이것을 확인할수 있다.

SNMP지원

단순망관리규약(SNMP)은 Cisco경로기에 대한 통계들을 수집하고 구성변화를 만들기 위하여 리용될수 있다. 이것은 공동체문자렬의 리용에 의하여 수행된다. 간단히 말하여 공동체문자렬은 한 장치에 대한 특정의 접근준위(읽기전용 또는 읽기-쓰기)를 식별하는 통과암호체계이다.

실례로 대부분의 장치는 그 장치에 대하여 읽기전용접근을 허용하는 Public라는 공동체문자렬을 사용하도록 미리 예비구성되여 있다. 이 공동체문자렬을 리용하여 SNMP를 통하여 그 경로기에 접근하는 사람은 자동적으로 접근이 허가된다.

인증이 약한것외에 SNMP는 또 하나의 주요한 보안약점을 가진다. 그것은 모든 정보를 평문으로 전송한다는것이다. 망을 감시하던 사람은 통과하는 자료흐름으로부터 공동체이름을 가로챌수 있다.

SNMP는 또는 전송규약으로 UDP를 사용한다. 제5장에서 본바와 같이 UDP는 그것의 비련결성으로 하여 려파하기 매우 어렵다.

이러한 리유들로 하여 가능하다면 자기의 경로기에서 SNMP를 리용하는것을 피하여야 한다. 관리가능성은 큰 환경에서는 실제적인 리득일수 있지만 경로기에 들어 가는 이 뒤문은 엄중한 보안문제를 초래할수 있다.

일러두기

만일 SNMP를 리용하여야 한다면 SNMPv2을 리용하시오. 이 최신판본은 MD5인증을 지원하여 보안을 개선시킨다. 이 보안은 간단한것은 아니고 원래의 SNMP보다 훨씬 좋다. Cisco경로기판본 10.3 이상은 SNMPv2를 지원한다.

구성파일을 지키기

Cisco경로기의 구성은 다음의 지령을 입력하여 볼수 있다.

write term 또는 show running-config

구성파일은 TFTP규약을 리용하여 원격봉사기에 복제될수도 있다. Cisco경로기파일의 표본머리부를 아래에 보여 준다.

```
! Cisco router configuration file
hostname lizzybell
enable secret 5 $ 1 $ 722 $ CE
enable password SuperSecret
line vty 04
password SortaSecret
!
```

특권방식(enable)통과암호는 한방향암호화알고리듬을 리용하여 암호화된다. 그러므로 구성파일을 보는 사람은 이 통과암호를 즉시 리해하지 못한다. enable password문자렬은 그저 뒤방향호환성을 위하여 리용된다. 만일 이 구성파일이 암호화된 통과암호를 지원하지 않는 이전의 경로기에 틀리게 적재된다면 이 통과암호는 암호화된것 대신에 리용된다.

그러나 telnet대화통과암호들은 평문으로 되여 있으므로 이 파일은 가능한껏 엄밀히 지켜야 한다. 만일 이 파일이 TFTP를 통하여 적재된다면 그 망을 감시하는 공격자는 지금 이 장치를 접근하는데 필요한 첫 통과암호를 가진것으로 된다. 이 정보를 더잘 지키기 위하여 전체 구성방식에서 다음의 지령을 입력함으로써 모든 통과암호들을 암호화할수 있다.

```
Service password-encryption
```

이것은 모든 통과암호문자렬들의 기억기복사본을 암호화한다. 이것을 영구적인것으로 만들기 위해서는 다음과 같이 입력하여 그 변화를 보관하여야 한다.

```
write term
```

또는

```
copy running-config startup-config
```

모든 통과암호문자렬들이 지금 암호화되였지만 아직도 구성파일을 안전하게 하기 위한 예방조치를 더 취해야 한다. 암호화된 문자렬을 사전파일에 있는 항목들과 비교함으로써 통과암호의 값을 알아 내려고 시도하는 크래커프로그람들이 존재한다. 어떤 하나가 맞는다면 그 통과암호에 등가한 평문이 얻어 진다. 이러한 형태의 공격을 막기 위한 유일한 방법은 암호화된 통과암호문자렬들이 나쁜 손에 들어 가지 않도록 하는것이다.

속임수로부터의 보호

공격자는 속임수를 써서 방화벽의 안전한 쪽으로부터 오는것처럼 보이는 하나의 파케트를 전송할수 있다. Cisco경로기에서 속임수를 막는 몇가지 방법들이 있다.

- 접근목록의 사용자료흐름이 알려 진(또는 기대되는) 원천주소로부터 올 때에만 통과시키는 모든 대면부들에서 입구접근목록을 만든다. 모든 다른 자료흐름은 거절된다.

• 불가능한 원천경로조종: 원천경로조종이 모든 대면부들에서 불가능으로 되여야 한다.
• 작은 봉사들은 꺼버리기: 이러한 봉사들은 대부분의 망기반구조들에서 보통 중요하지 않으나 악용될 가능성이 있다. 지령 no service tcp-small-serves가 IP통신에서 이것들을 꺼버리는 하나의 실례이다.

방향 가진 방송을 금지하기

DoS(봉사거부)공격은 목표콤퓨터에 많은 정보(또는 많은 련결요청)가 넘쳐 나게 함으로써 그 목표가 합법적인 요청에 봉사할수 없게 한다. 이러한 형태의 공격에 해커들이 리용하는 도구들중의 하나는 방향 가진 방송을 전송하는 경로기의 능력이다. 방향 가진 방송들을 불가능으로 하기 위하여 다음의 지령을 입력한다.

no ip directed broadcast Routing

기정에 의하여 Cisco경로기들은 IP경로조종이 가능으로 되여 있고 당신은 이 기능을 변경시킬수 없다. 그러나 자기의 내부망에서 어느 부분망을 돌리고 있는가를 고려하여 어떻게 하면 자기의 경로기를 가장 잘 갱신할것인가를 고려하여야 한다. 경로기는 자동적으로 국부적으로 련결된 망들에 대하여 알고 있다. 그뒤에 있는 어떤 부분망에 도달하기 위하여서는 경로기에 어떻게 거기에 도달할것인가를 구체적으로 알려야 한다.

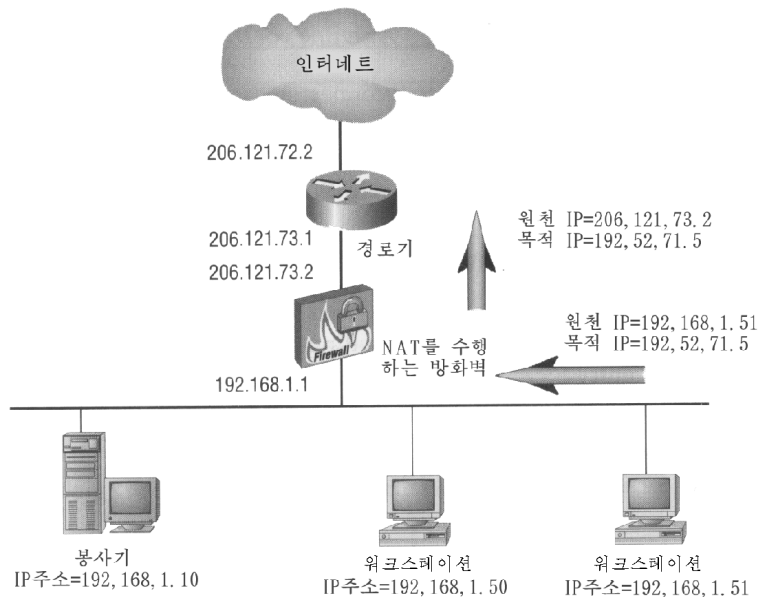



그림 6-1. 방화벽이 NAT를 수행하고 있으므로 우리의 경로기는 내부망에 대한 경로항목을 알 필요가 없다

때로 이것은 문제로 되지 않는다. 실례로 그림 6-1을 보기로 하자. 우리의 방화벽은 내부망을 위하여 망주소변환(NAT)을 수행하고 있다. 경로기가 보는 모든 자료흐름은

국부적으로 부속된 토막으로부터 오는것처럼 나타날것이다. 이 경우에 기정의 경로기를 넘어서 어떤 다른 경로항목이 요구되지 않는다. 우리는 NAT를 리용하고 있으므로 경로기는 192.168.1.0에 대하여 알 필요가 없다.

만일 경로기가 알아야 할 추가적인 부분망을 가지고 있다면 그 경로기에 정적항목을 만들것인가(정적경로조종) 또는 경로기가 경로정보를 자동적으로 받도록 하기 위하여 RIP나 OSPF과 같은 동적규약을 리용할것인가(동적경로조종) 하는것을 결정하여야 한다. 매 선택에는 구성에 따라 우점과 약점이 있다.

정적경로조종은 보안의 견지에서 보다 안전하다. 만일 경로기가 이미 어떤 경로구성으로 프로그람화되였다면 공격자는 그 경로기를 손상시킴이 없이는 이 정보를 변화시킬수 없다. 만일 동적규약이 리용된다면 공격자는 틀린 갱신의 내용을 경로기에 보내여 경로표를 혼란시킬수 있다. 동적경로조종은 같은 망에서 여러개의 경로들을 운영하고 있다면 유용하다. 실례로 만일 인터네트에로 가는 여러개의 련결을 가지고 있다면 여유 또는 부하균형을 위하여 동적경로조종규약을 사용하는것이 리로울수 있다. 만일 동적경로조종규약을 리용하여야 한다면 OSPF와 같은 인증을 지원하는것을 리용하는것이 좋다. 이것은 적어도 일정한 정도의 보안을 제공할것이다. RIP와 같은 경로조종규약은 그저 경로정보를 보내는 호스트가 그것이 무엇에 대하여 말하고 있는가를 알아야 한다는것을 믿고 있다.

주　의

동적경로조종에 대하여서는 제3장을 보기 바란다.

리용중에 있는 인터네트련결의 대부분은 그 기관과 그의 ISP사이에 하나의 련결만을 가지고 있다. 이러한 환경에서는 정적경로조종이 적합하다. 경로조종표를 수동적으로 작성하는데 드는 약간의 유지비증가는 추가적인 보안을 위하여 필요한것으로 볼수 있다.

정적경로조종의 구성

최소로 자기의 경로기를 기정의 경로기설정으로 구성하여야 한다. 기정의 경로기설정은 다음과 같이 말하는것이다. 《만일 당신이 특정의 부분망에 대한 경로표항목을 가지고 있지 않다면 그 자료를 이 다른 경로기에 전송하고 그 경로기로 하여금 그것을 어떻게 배달할것인가를 판단하게 하시오.》 기정의 경로는 WAN련결의 다른 끝에서 ISP의 경로기를 리용하도록 구성되여야 한다.

기정의 경로는 전체 구성방식에 들어 가서 다음의 지령을 입력하여 구성할수 있다.

```
ip default-route xxx.xxx.xxx.xxx
```

여기서 xxx.xxx.xxx.xxx는 기정경로기의 국부IP주소이다. 일단 기정경로를 만들었다면 합법적인 주소들을 리용하는 매 내부부분망들에 대하여 정적경로들을 넣어야 할것이다. 역시 전체 구성방식에서 다음의 지령을 입력한다.

```
ip route yyy.yyy.yyy.0 255.255.255.0 xxx.xxx.xxx.xxx 1
```

이것을 추가하려고 하는 매 부분망들에 대하여 한번씩 하여야 한다. 이 지령은 다음

과 같이 해석할수 있다.

ip route: 정적IP경로항목을 첨가하시오.
yyy.yyy.yyy.0: 이 값을 IP부분망주소와 교체하시오.
255.255.255.0: 이 값을 정당한 부분망마스크주소와 교체하시오.
xxx.xxx.xxx.xxx: 이 값을 다음 도약경로기의 IP주소와 교체하시오.
1: 이것은 이 경로를 따라 가는것과 관련한 거리 또는 비용이다. 같은 목적지에로의 여러개의 경로를 가지고 있지 않는 한 1값을 리용하시오. 여러개인 경우에는 가장 바라는 경로는 1로 설정하고 그 다음경로는 2로 설정하면 된다.

이것이 어떻게 구성되는가를 보기 위하여 한가지 실례를 고찰하자. 그림 6-2를 보면 구성하려는 환경에 여러개의 경로기가 있다는것을 알수 있다.

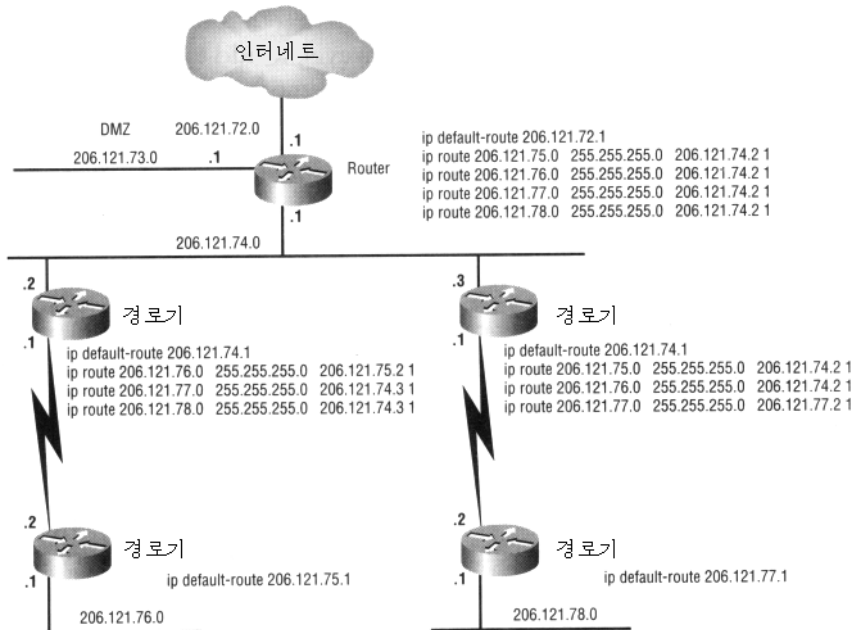



그림 6-2. 여러 경로기에서 정적경로들을 정의하기

매개 경로기는 기정의 경로설정을 가지고 있다. 만일 망(206, 121, 76, 0 또는 206, 121, 78, 0)의 제일 뒤에서 출발한다면 기정의 경로항목들은 모두 인터네트에로 향한다는것을 볼수 있다. 이것은 좋은 일이라고 볼수 있다. 왜냐하면 우리의 경로기에로 프로그람화되는것을 피하려고 하는것이 인터네트밖의 모든 부분망들이기때문이다. 기정의 경로는 정의되지 않은 경로에 대하여 포괄적인것으로서 작용한다.

주 의

그림 6-2에서 두개의 가장 멀리 있는 경로기들은(206, 121, 75, 1과 206, 121, 77, 2) 기정의 경로만을 리용하고 있다. 여기에는 정적경로항목이 없다. 이것은 이 장치에 직접 붙어 있지 않는 부분망에 도달하기 위하여서는 기정경로기를 통과시키려 하기때문이다. 정적경로항목들을 첨가할수 있지만 그것들은 여분으로 된다.

마지막으로 DMZ에 대해서는 우리의 경로기들에 경로항목을 하나도 첨가하지 않았다는것을 주목하여야 한다. 이것은 그것이 필요하지 않기때문이다. 우리의 인터네트경로기는 이 토막에 직접 붙어 있으므로 어떻게 거기에 가야 하는가를 이미 알고 있다. 다른 경로기들에서와 같이 DMZ도 간단히 기정의 경로항목을 리용하여 도달할수 있다.

원천경로조종

우리는 이제 하나의 최종적인 경로항목을 만들어야 한다. 대표적으로 IP파케트들은 경로정보를 포함하지 않는다. 파케트들은 최량의 경로를 선택하는것을 망경로조종하드웨어에 맡긴다. 그러나 원격체계에 접근할 때 취하려고 하는 경로를 머리부정보에 첨가하는것이 필요하다. 이것을 원천경로조종이라고 부른다.

경로기가 하나의 원천경로파케트를 받을 때 그는 머리부에서 정의된 다음번 도약에로 그 정보를 전송한다. 그 경로기가 원격체계에로 도달하는 보다 좋은 경로를 알고 있다고 해도 그것은 파케트머리부안의 경로지정에 따른다. 대표적으로 원격체계가 하나의 원천경로파케트를 수신할 때 그것은 같은 지정된 경로에 따라 그 요청에 응답할것이다.

원천경로조종은 망에 있는 잠재적인 뒤문을 악용하려고 하는 공격자에 의하여 리용될수 있다. 실례로 회사가 어떤 적당한 방화벽을 설치하는데 많은 시간과 돈을 투자하였다고 하자. 회사는 자기의 인터네트련결을 될수록 든든히 잠그기 위하여 많은 노력을 기울였다.

또한 회사가 방화벽뒤에서 자기의 망에 련결하는 원격기업상대와 하나의 WAN련결을 가지고 있다고 가정하자. 이 기관도 인터네트련결을 가지고 있는데 거기에는 보안에 대한 모든 선전이 방화벽제작자들의 시장책략이라고 생각하지 않는 사람들로 구성되여 있다. 그러므로 기업상대는 자기의 망방어선에 대한 보호를 가지고 있지 않다.

원천경로파케트를 리용하면 잠재적인 공격자가 먼저 원격기업상대에게 자료흐름을 보내고 다음에 자료파케트안에 있는 원천경로정보를 리용함으로써 그 자료흐름이 WAN련결을 통하여 회사의 망에로 전송되게 할수 있다. 모든 보안노력에도 불구하고 공격자는 회사의 망환경에 들어 가는 쉬운 접근통로를 찾아 내였다.

원천경로조종은 해로운것일수 있으며 모든 망환경에서 불가능으로 되여야 한다. 원천경로파케트를 허용하는 유일한 합법적인 리유는 인터네트우의 특정한 련결에 대한 련결성진단을 하려고 할 때 필요하다는것이다. 이것은 우리가 해야 할 일중에서 큰 부분이 아니므로 그 기능은 불가능으로 해놓는것이 제일 좋다.

원천경로조종을 불가능으로 하기 위해서는 전체 구성방식에 들어 가서 다음의 지령을 입력한다.

```
no ip source-route
```

Cisco보안의 특징

표 6-3은 Cisco IOS에서의 여러가지 보안상 특징들에 대한 목록을 제공한다(일부는 가장 최근의것이다.).

표 6-3 Cisco IOS보안특징

특 징	설 명
표준접근목록과 정적 확장접근목록	망층에서 파케트평가에 의한 기초려과를 가능하게 한다(어떤 확장접근목록들은 전송층에서도 정보를 평가할수 있다.).
동적접근목록 (자물쇠-열쇠라고도 한다.)	인증된 사용자에게 림시접근을 제공한다.
반사적접근목록	들어 오는 TCP 또는 UDP파케트들이 방화벽안쪽에서 시작된 대화에 속한다면 그것들을 허용한다.
TCP차단	SYN범람공격(DoS공격의 한 형태)으로부터 보호한다.
문맥에 기초한 접근조종	필요할 때 련결들을 동적으로 열거나 닫기 위하여 응용층정보들을 검사하여 모든 TCP와 UDP련결들의 상태가 아니라 문맥을 결정한다. 또한 경고와 등록에 응답가능하다.
침입검출	모든 망자료흐름을 지정된 징후와 비교한다. 침입이 검출되면 경보를 내고 련결을 재설정하거나 차단한다.
인증대리자	사용자에 기초한 접근방책들을 적용한다(집단 또는 IP에 기초한 접근방책에 대립하는것으로서).
포구/응용프로그람의 사상	문맥에 기초한 접근조종이 등록되지 않은(규격화되지 않은) 또는 주문포구들에서 작업하는것을 가능으로 한다.
NAT	사설IP주소들을 공개인터네트로부터 숨긴다.
사용자인증 및 권한주기	사용자구좌에 기초하여 신분 및 허용준위를 확인한다.

이 모든 보안방법들의 핵심부에는 접근목록이 있다. Cisco접근목록 (려파기라고도 부른다.)들은 Cisco경로기가 수신한 자료흐름을 선택적으로 통과 또는 차단하는데 리용된다. 경로기는 수신된 매 파케트를 정보의 원천 또는 목적지주소, 웃층의 규약, 시간, 사용자신분 등과 같은 접근목록에서 정의된 규준들에 따라 평가한다.

접근목록은 망경계선을 통과하려고 하는 자료흐름을 조종하는데서 유용하게 쓰인다. 경로기는 전형적으로 망토막들을 격리 또는 분할하는데 리용되므로(실례로 망을 기업상대 또는 인터네트로부터 분리하는것) 독자는 왜 이 장치들이 고급한 려파기능을 가지고 있는가를 알수 있을것이다.

Cisco경로기는 자료흐름을 려파하는 두가지 방법을 제공한다. 가장 간단한것은 표준접근목록이고 보다 세밀한 조종을 위하여서는 확장접근목록이 리용된다.

하나의 접근목록이 만들어 지면 그것은 그 경로기의 어느 특정의 대면부에 적용된다. 이때 접근목록은 들어 오는 망자료흐름(부속된 망으로부터 그 대면부에로 오는) 또는 나가는 망자료흐름(그 경로기를 떠나 부속된 망에로 가는)을 하나씩 조사할수 있다.

들어 오는 또는 나가는 자료흐름을 려파하는 능력은 복잡한 구성에서 실제적인 시간절약기로 될수 있다.

Cisco IOS 12.1에서 IP와 IPX확장접근목록이 시간대역에 따라서도 리용될수 있다. 허용 또는 거부통보문이 그것들이 련관된 시간대역에 따라 활성화된다. 다른 우점들은 다음과 같다.

증가된 조종 자원(IP주소/마스크쌍, 포구번호, 경로조종방책 또는 요구에 따르는 련결만들기)들은 준비된 시간에 련결된다.

더 좋은 통합 시간에 기초한 방책은 Cisco의 방화벽 및 IPSec제품들과 련결될수 있다.

비용의 감소 자료흐름은 시간에 기초하여 보다 적은 비용으로 다시 경로조종될수 있다.

효과성증대 접근목록은 그날의 열린 시간에 처리되지 말아야 한다.

시간대역을 만들기 위하여 다음의 지령을 리용한다.

time-range {name of time range}

실제적인 시간대역을 정의하기 위해서는 다음의 지령을 입력한다.

Periodic {days of the week} {hh：mm} to {days of the week} {hh：mm}

접근목록의 기초

접근목록은 목록식별자번호들과 련관되는 많은 검사조건들을 만듦으로써 형성된다. 접근목록은 전체 구성방식에서 다음의 문법을 리용하여 창조한다.

access-list {list #} permit/deny {test condition} {time range}

자료흐름을 골라 내는데 리용하려고 하는 매 검사조건들(SMTP는 허용하고 HTTP는 거부하는 등의)에 대하여 이 지령을 반복한다. 리용하는 목록번호는 어느 규약에 이 규칙들을 적용하려고 하는가를 식별한다. 표 6-4는 이름과 관련된 규약들을 보여 주며 표 6-5는 목록번호와 관련된 규약들을 보여 준다.

표 6-4 이름에 의한 Cisco접근조종목록들

규 약
Apollo Domain
IP
IPX
ISP CLNS
NetBIOS IPX
Soure-route Bridging NetBIOS

주 의

어떤 규약들은 자기들의 련관목록표가 이름에 의해서만 또 다른것들은 번호에 의해서만 식별될것을 요구한다.

표 6-5　　　번호에 의한 Cisco접근조종목록의 표본

규　약	목 †형식	대역식별자
IP	표준	1-99;1300-1999
IP	확장	100-199;2000-2699
Ethernet Type codes	N/A	200-299
AppleTalk	N/A	600-699
Ethernet Addresses	N/A	700-799
IPX	표준	800-899
IPX	확장	1000-1099

어떤 규약들에서는 한가지 려과형태만이 지원된다는것을 알아야 한다. Cisco IOS 11.2와 그이상급들에서처럼 IP에 의하여 리용되는 대역식별자들은 기호적인 이름으로 교체될수 있다. 이 이름은 64문자만큼 길수 있는데 첫 기호는 문자여야 한다. 이름은 일의적이여야 하며 매개 이름은 하나의 표준 또는 확장려과기모임을 지적하여야 한다. 두개를 결합할수는 없다. 접근목록이름을 만드는 문법은 다음과 같다.

IP access-list standard/extended {name}

일러두기

접근목록번호대신 이름을 리용하면 매우 유리하다. 그렇게 하면 만들수 있는 일의적인 목록의 수를 확장할수 있고 서술적이름을 특정의 려과기모임과 련결시킬수 있다. 또한 재귀려과기들은 접근목록이름과만 련결될수 있다. 접근목록식별자번호를 사용할수 없다.

접근목록들은 그것들을 만드는 순서로 처리된다. 만일 5개의 려과기조건들을 만들고 그것들을 같은 접근목록에 넣는다면 경로기는 첫번째 맞춤이 얻어 질 때까지 그것이 만들어 진 순서로 매 조건들을 평가한다. 조건들은 《가장 잘 맞음》이 아니라 《첫번째 맞춤》으로써 처리되며 따라서 리용하는 순서에 주의를 돌리는것이 중요하다.

실례로 다음과 같은 접근목록을 가지고 있다고 가정하자.

- 모든 내부체계들에 인터네트에로의 완전한 IP접근을 허용한다.
- 어떤 내부체계도 인터네트우에 호스트들에서 telnet를 할수 없다.

첫번째 규칙은 《모든 밖으로의 자료흐름은 허용된다.》이므로 이것을 두번째 규칙에 맞출수 없다. 이것은 내부사용자들이 아직 telnet를 리용할수 있다는것을 의미한다.

일단 자기의 경로기에 적용하려고 하는 접근표를 만들수 있다면 특정의 대면부를 위한 구성방식에 들어 가서 다음의 지령을 입력하면 된다.

{protocol} access-group {list # or name} in/out

어떤 대면부로부터 하나의 접근목록을 제거하기 위하여서는(새로운 려과기를 시험하고

있을 때 흔히 하는것) 간단히 그 지령앞에 단어 no를 붙이면 된다.

no {protocol} access-group {list # or name} in/put

마찬가지로 전체 접근표를 지우려면 다음의 지령을 입력한다.

no access-list {list # or name}

이것은 특정의 접근목록번호 또는 이름과 련관된 모든 려과기조건들을 지우게 된다. 접근목록의 가장 큰 결함의 하나는 사용자가 항목들을 편집할수 없다는것이다. 이것은 자료항목들이 좀 장황하게 되게 한다. 실례로 15개의 접근목록항목들을 만들었는데 실제로 항목 13후에 항목 11를 처리하여야 한다는것을 알았다면 전체 목록을 지우고 그것을 처음부터 다시 만들어야 한다.

일러두기

접근표를 본문편집기에서 따로 만들자. 정확한 순서로 되여 있는 려파기들을 가지고 있다면 간단히 그 규칙들을 Windows의 오려둠판에 복사하고 말단모방기의 붙이기기능을 리용하면 된다. 그러면 자기의 모든 려파기조건들은 국부적여벌복사를 가지게 된다.

모든 접근려과기들은 그끝에서 하나의 무조건적인 거부를 가지고 있다. 이것은 경로기에 어떤 형식의 자료흐름을 통과시키라고 구체적으로 지적하지 않는다면 그것은 차단될것이라는것을 의미한다. 실례로 만일 접근목록이 《부분망 192.168.1.0에서 오는 자료흐름은 통과시키시오.》라고 되여 있다면 경로기는 192.168.1.0을 제외한 모든 부분망들로부터 오는 자료흐름을 차단하여야 한다고 가정할것이다. 이러한 특징은 의도하지 않은것은 그 어느것도 할수 없도록 담보하는데서 도움이 된다.

표준접근목록

표준접근목록은 원천IP주소상에서 려과하게 하는것이다. 이것은 어떤 특정의 부분망 또는 호스트로부터의 모든 자료흐름을 차단하려고 할 때 유용하다. 표준접근목록은 목적지IP주소 또는 그 봉사까지도 보지 않는다. 그것은 전송하는 체계의 원천주소안에 의거하여 려과결정을 한다.

이것은 좀 제한성이 있으나 사실상 매우 유용할수 있다. 그림 6-3을 보자. 여기서는 하나의 매우 간단한 망설계를 볼수 있다. 망의 안으로 및 밖으로 유일한 하나의 길만이 있는데 그것은 경로기를 통하게 되여 있다. 내부망토막은 IP부분망주소 206.121.73.0을 리용한다.

이 환경에서 경로기는 IP부분망 206.121.73.0으로부터 오는것으로 나타나는 자료는 보지 말아야 한다. 그것은 그 망토막이 경로기의 그 이써네트포구에 직접 련결되여 있기때문이다. 경로기는 자기의 이써네트포구의 이 부분망으로부터 오는 자료흐름을 보고 있지만 그것은 직렬(WAN)포구의 밖에서는 검출되여서는 안된다.

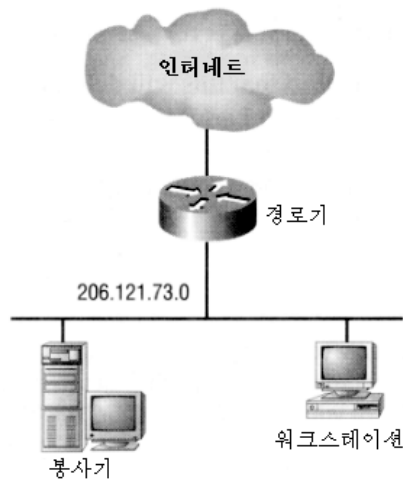



그림 6-3. 표준접근목록의 리용

IP속임수(spoofing)는 공격자가 어떤 먼 위치에 떨어 져 있으면서도 정보를 전송하는 기관의 국부망의 한 체계인것처럼 가장하는것이다. 이것은 체계의 어떤 취약성을 악용하여 진행할수 있다. 실례로 Microsoft Windows는 랜드(Land)라고 알려 진 공격형태에 취약하다. 랜드공격파케트는 다음의 속성들을 가진다.

원천IP 공격되는 체계의 IP주소
목적지IP 공격되는 체계의 IP주소
전송층 TCP
원천포구 135
목적지포구 135
기발설정 SYN=1

다른 포구들과 설정들이 리용될수 있으나 여기서는 일반적인 내용만을 주기로 한다. 공격자는 체계가 자기자신과 대화하고 있는것처럼 생각하도록 속인다. 이것은 그 어떤 경주조건을 만들어 내는데 결과적으로 체계는 정지되거나 차단된다.

이렇게 생각할수 있다. 《문제가 없다. 나는 들어 오는 모든 요청들을 차단하려고 한다. 그렇게 하면 이 파케트는 SYN기발이 1로 설정되여 있기때문에 결코 통과하지 못할것이다.》

그렇지 않다. 원천주소를 보라. 경로기가 이 파케트를 평가할 때 그것은 분명 그 파케트가 내부망으로부터 수신되였다고 생각할수 있다.

Cisco경로기들은 이 문제를 가지고 있지 않으나(그것들은 그 파케트와 그것이 수신된 대면부와의 결합을 유지하고 있다.) 많은 경로기들은 문제가 있다. 만일 접근규칙이 《내부망으로부터 오는 포구135는 통과시키시오.》라고 되여 있다면 경로기는 그 자료파케트를 좋다고 보고 그 정보를 경로조종과정을 따라 통과시키는데 그러면 그것은 이써네트토막을 따라 통과되게 된다.

그러면 어떻게 이 문제를 풀것인가? 내부부분망주소를 리용하여 인터네트로부터 오는 합법적인 자료흐름을 결코 보지 못할것이므로 이러한 자료흐름들을 려과한다면 련결에서 손실은 없을것이다. 이것을 속임수려과기(spoofing filter)라고 부른다. 그것은 왜냐하면 기관의 망주소로 가장하려고 하는 자료흐름들은 통과하지 못하도록 담보하고 있기때문이다.

다음과 같은 규칙을 가지는 내부 방향려과기를 이써네트포구에 배치하는것도 좋은 생각이다. 《206.121.73.0부분망으로부터 오는 자료흐름만 허용하시오.》 이것은 내부사용자들이 다른 망에 대한 속임수공격을 시도하지 못하도록 담보하는데 도움이 된다. 관리자로서 자기의 환경을 보호할뿐아니라 부주의로 다른 사람의 생활을 불행하게 만들지 않도록 담보하는것도 하여야 할 일감으로 된다.

표준접근목록을 리용하여 속임수려과기를 만들수 있다. 표준접근목록의 항목에 대한 문법은 다음과 같다.

```
access-list {list # or name} permit/deny {source} {mask}
```

그림 6-3의 경로기에서 전체 구성방식에서 다음과 같은 접근목록항목들을 만들수 있다.

```
Access-list 1 deny 206.121.73.0 0.0.0.255
Access-list 2 permit 206.121.73.0 0.0.0.255
```

접근목록 1은 WAN대면부에 대한 구성방식에 들어 가서 다음의 지령을 입력함으로써 적용된다.

```
ip access-group 1 in
```

마찬가지로 접근목록 2는 이써네트대면부에 대한 구성방식에 들어 가서 다음의 지령을 입력하여 적용한다.

```
ip access-group 2 in
```

마스크값이 좀 이상하다고 생각할수 있다. 이것은 이 값이 부분망마스크가 아니라 패턴정합이기때문이다. 패턴정합은 하나의 검사조건을 평가할 때 다음의 규준을 리용한다.

0: 정의된 주소에서 해당byte는 검사조건과 정확히 맞아야 한다.
1: 이것은 예측할수 없는 문자이다. 이 byte에서의 어떠한 값도 맞는것으로 인정한다.

그러므로 이 실례에서 우리의 패턴정합은 《byte값 206.121.73을 포함하는 임의의 IP주소》라고 말하는것으로 된다. 첫 3byte가 원천IP주소와 맞는 한 접근목록검사조건은 그것을 맞는것으로 인정한다.

모든 망자료흐름을 맞도록 하기 위해서는 다음의 주소와 마스크를 리용한다.

0.0.0.0 255.255.255.255

이것은 Cisco경로기에서 모든 자료흐름이 다 정합되는것으로 간주된다고 말하는것으로 된다. 자기의 접근규칙들을 쓸 때 이 주소와 마스크는 단어《임의의 (any)》에 의하여 교체될수 있다. 이것은 표준접근목록에 대해서는 그리 유용하지 못하지만(만일 어떤

자료흐름도 받아 들이기를 원치 않는다면 간단히 접속구를 뽑는것이 더 쉬울것이다.) 이제 다음절에서 확장접근목록을 론의할 때에는 여러모로 쓸모가 있을것이다.

접근목록패턴정합

패턴정합값을 《반부분망마스크》로 생각한다면 그것은 아주 잘 리해한것이라고 볼수 있다. 패턴정합은 항상 부분망마스크에 리용된것과 정확히 반대값이다. 이것은 완전부분망류형들을 려과하고 있다면 리해하기 매우 쉽지만 실제적인 부분망들을 가지고 일하고 있다면 좀 혼돈이 생길수 있다.

실례로 완전한 류형 C망대신에 이 류형 C주소공간의 한 부분만을 리용하고 있다고 하자. 망주소는 206.121.73.64이고 부분망마스크는 255.255.255.224라고 가정하자. 이 경우에 패턴정합을 위하여 무엇을 리용하여 자기의 망공간에서만 려과하고 있다는것을 담보하겠는가?

모든 TCP/IP주소공간은 사실상 2진수체계를 리용하여 만들어 진다. 그렇지만 편리상 현재 10진수를 리용하여 표시하고 있다. 자기가 리용할 패턴정합을 결정하기 위하여 먼저 부분망마스크의 마지막 byte를 2진수로 변환하여야 한다.

224 = 128 + 64 + 32 = 11100000

마지막 byte에서 3bit는 망을 위하여 사용하고 다섯비트는 매 호스트를 일의적으로 식별하는데 사용하고 있다. 망에서 어떤 호스트를 무시하기 위하여 모든 호스트비트들을 1로 설정하는 패턴정합을 리용한다.

00011111 = 16 + 8 + 4 + 2 + 1 = 31

그러므로 새로운 망주소와 부분망마스크를 적응시키기 위하여 다음의것으로 접근을 변경시켜야 한다.

```
Access-list 1 deny 206.121.73.64 0.0.0.31
Access-list 2 permit 206.121.73.64 0.0.0.31
```

결국 자기의 접근목록에 다음과 같이 말하는것으로 된다. 《주소공간값 206.121.73.64−206.121.73.95(64+31)을 볼 때 그 파케트를 려과하시오.》 이렇게 하면 필요한것 이상을 려과하거나 허용함이 없이 이 류형 C주소공간의 작은 부분을 선별할수 있다.

속임수규칙들을 제외하고 또 무엇때문에 표준접근목록을 리용하는가? 표준접근목록은 어떤 달갑지 않은 원격싸이트로부터의 접근을 막는데 매우 효과적이다. 이것은 공격자일수도 있고 스팸우편물제공자일수도 있으며 또는 경쟁자일수도 있다.

인터네트에 련결하였다고 하여 모든 원천으로부터 오는 자료들을 다 받아야 한다는 요구는 없다. 모든 자료흐름을 다 받아 들이는것이 고상한 행동으로 간주될수 있으나 그것이 항상 기업의 견지에서 좋은것은 아니다.

실례로 스팸싸이트를 식별하기 위한 전용자원을 가지고 있는 우편목록과 기관들이 있다. 스팸 또는 불필요한 광고전자우편은 좋게 보아서 자원의 랑비이며 나쁘게는 봉사

거부를 초래할수 있다. 많은 관리자들은 지금 스팸을 지원(또는 적어도 그것을 막는데 실패)한다고 알려 진 싸이트들로부터의 자료흐름을 려파하고 있다. 나가는 스팸우편을 조종하지 못하는 싸이트는 망에 대한 다른 형태의 공격도 막지 못하므로 그것의 모든 자료흐름은 려파된다.

일러두기

Cisco대면부는 포구당, 방향당 하나의 접근목록만을 허용할수 있다. 이것은 확장접근목록을 필요로 하지 않을 때 표준접근목록을 적용하여야 한다는것을 의미한다. 만일 확장접근목록의 좋은 유연성이 필요하다면 간단히 자기의 려파기를 하나의 목록에 련결시키는것이 좋다.

정적확장접근목록

확장접근목록은 표준접근목록보다 한걸음 더 전진한 개념을 사용한다. 원천IP주소우에서 간단히 려파할 대신에 확장접근목록은 다음의 내용들에 따라 려파할수 있다.

- 목적지IP주소
- 전송층(IP, TCP, UDP, ICMP, GRE, IGRP)
- 목적지포구번호
- 파케트형식 또는 ICMP의 경우에 코드
- 설정된 련결(ACK 또는 RST비트가 설정되였는가를 검사)

명백히 이것은 주위의 자료흐름들에 대한 보다 세밀한 조종준위를 부여할수 있다. 확장접근목록은 전체 구성방식에서 다음의 문법으로 만들어 진다.

Access-list {list # or name} permit/deny {protocol} {source} {mask } {destination} {mask} {operator} {post} est (short for establish if applicable)

연산자들은 다음과 같다.

lt : 보다 작다
gt : 보다 크다
eq : 같다
neq : 같지 않다

한가지 실례로서 호스트 206.121.73.10우의 HTTP에로의 열린 접근을 허용하고 telnet접근도 허용하지만 부분망 199.52.24.0의 호스트로부터의 접근만을 허용하지 않는 확장접근규칙들의 모임을 만들려고 한다고 하자. 이 규칙들은 다음의것과 류사하게 볼수 있다.

```
access-list 101 permit any 206.121.73.10 0.0.0.0 eq 80
```

```
access-list 101 permit 199.52.24.0 0.0.0.255 206.121.73.10 0.0.0.0 eq 23
```

다음에 그 대면부에 대한 구성방식에 들어 가서 다음의 지령을 입력함으로써 이 규칙들을 직렬포구에 설치할수 있다.

```
ip access-group 101 in
```

FTP와 관련한 문제들

제3장에서 FTP에 대하여 본바와 같이 이 규약은 방화벽을 통하여 지원하기가 매우 어렵다. 그것은 이 규약이 파일을 전송하는 동안 두개의 포구를 리용하기때문이다. 간단히 다시 고찰해 보자.

표준FTP 1023우의 모든 들어 오는 봉사포구는 자료련결을 지원하기 위해 열려져 있어야 한다.

피동FTP 1023우의 모든 나가는 봉사포구는 자료련결을 지원하기 위해 열려 져 있어야 한다.

두개의 나쁜것중 작은것을 택한다는 의미에서 보통 피동FTP만을 지원하는것이 더 좋다. 이것은 모든 Web열람기들과 대부분의 도형식FTP프로그람들에서 지원된다. 명령행식 FTP프로그람들에서는 대체로 지원되지 않는다.

피동FTP를 지원하기 위하여서는 모든 내부호스트들에 인터네트를 위한 체계의 1023우의 임의의 TCP포구들에 접근하는것을 허용하여야 한다. 그것은 가장 좋은 보안자세는 아니지만 표준FTP보다는 좋다.

기관이 막으려고 하는 특정의 봉사들이 있다면 모든 나가는 포구들을 열어 놓는 항목앞에 이 접근목록항목을 만들어야 한다. 규칙들은 순서대로 처리되므로 거부규칙들이 먼저 처리되고 그 자료흐름을 차단한다.

실례로 X11과 Open Windows봉사기에로의 접근은 막으려고 하고 피동FTP리용을 위하여 나머지 웃포구들은 열어 놓으려 한다고 하자. 이 경우에 다음과 같은 규칙들을 만들면 된다.

```
access-list 101 deny any any eq 2001
access-list 101 deny any any eq 2002
access-list 101 deny any any eq 6001
access-list 101 deny any any eq 6002
access-list 101 permit any any gt 1023
```

여기서 한가지 문제는 의뢰기가 포구 2001, 2002, 6001 또는 6002를 리용하려고 시도하였을 때 우연적인 FTP파일전송오유를 수신하게 된다는것이다. 이 오유는 흔히 일어나지는 않지만 발생한다면 처리하기 어렵다.

접근목록모임을 만들기

이 모든것이 어떻게 협력하여 일해 나가는가를 보기 위하여 한가지 실례를 고찰하자. 그림 6-4와 같은 망구성을 가지고 있다고 가정하자. Web봉사기에는 HTTP를 허가하고 우편봉사기에는 SMTP접근을 허용하려고 한다. 우편봉사기는 국부DNS과정도 돌린다. 또한 모든 TCP봉사에로의 제한없이 나가는 접근을 제공하려고 한다.

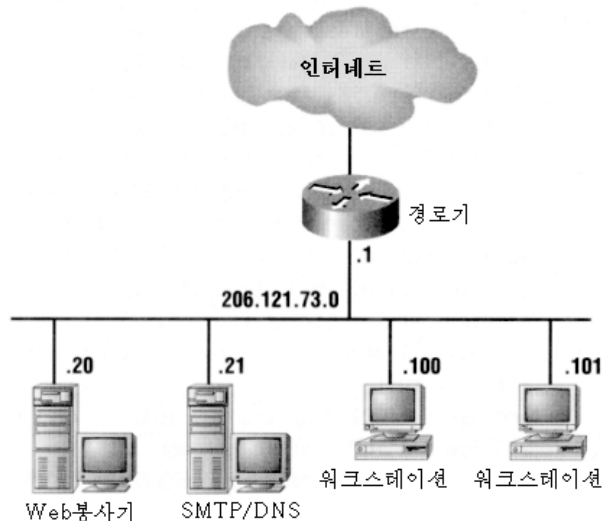



그림 6-4. 간단한 망에서 접근목록리용

접근목록규칙들은 다음과 같이 나타날것이다. 감탄부호(!)로 시작하는 행들은 Cisco IOS에서 설명으로 간주된다.

```
!stop any inbound spoofing
access0list 1 deny 206, 121.73.0 0.0.0.255
! Let in replies to established connection
access-list 101 permit tcp any 206. 121. 73.0 0.0.0.0.255 gt 1023est
! Look for port scanning
access−list 101 deny tcp any any eq 19 log
! Allo in SMTP mail to the mail server
access−list 101 permit tcp any 206.121. 73.21 0.0.0.0 eq 25
! Allow in DNS traffic
access−list 101 permit tcp any 206.121. 73.21 0.0.0.0 eq 53
access−list 101 permit udp any 206.121. 73.21 0.0.0.0 eq 53
! Allow in HTTP to the Web server
access−list 101 permit tcp any 206.121. 73.20 0.0.0.0 eq 80
```

```
! Let in replies if an internal user pings an external host
access−list 101 permit icmp any any echo−reply
! Allow  for  flow  control
acces−list 101 permit icmp any any source−quench
! Let in replies if an internal user runs traceroute
access−list 101 permit icmp any any time−exceeded
! Insure that our internal users do not spoof
access−list 2 permit 206. 121. 73.20 0.0.0.0.255
! Let out replies from the web server
access−list 102 permit tcp 206. 121, 73, 0.0.0.0 any gt 1023 est
!Let out replies from the mail/DNS server
acces−list 102 permit tcp 206.121.73.21 0.0.0.0 any gt 1023 est
! Let out DNS traffic from the DNS server
access−list 102 permit udp 206.121.73.21 0.0.0.0 any eq 53
! Block all other UDP traffic except for DNS permitted above
access−list 102 deny udp 206.121.73.0.0.0.0.255 any
! Allow a single host to create Telnet sessions to the router
acces−list 102 permit tcp 206.121.73.200 0.0.0.0.206.121.73.1 0.0.0.0 eq 23
! Block all oter hosts from creationg Telnet sessions
! to the router
access−list 102 deny tcp any 206.121.73.1 0.0.0.0 eq 23
! Allow all TCP traffic through
access−list 102 permit ip 206. 121.73.0 0.0.0. 255 any
```

이것이 전체 구성방식에서 입력되였다면 먼저 직렬대면부를 위한 구성방식에 가서 다음의 지령들을 입력한다.

```
ip access-group 1 in
ip access-group 101 in
```

다음에 이써네트대면부를 위한 구성방식에 가서 다음의 지령을 입력한다.

```
ip access-group 2 in
ip access-group 102 in
```

이것들을 끝내면 접근목록은 동작상태로 되고 경로기는 자료흐름을 려과하기 시작하여야 한다. 이때 자기의 구성을 즉시 검사하고 모든것이 기대되는대로 동작하고 있는가를 확인하여야 한다.

표본접근목록에 대한 몇가지 설명

세번째 접근목록의 이름은 《포구주사찾기》이다. 이것은 특정의 포구를 등록하여 모든 활동들이 조종탁말단에 연시되도록 함으로써 수행된다. 언급된바와 같이 경로기는 보통 매우 약한 등록능력을 가진다. 일반적으로 너무 많은 정보를 등록하기를 원치 않는다. 너무 많으면 그것을 붙잡기전에 화면에서 흘러 지나가고 말것이다. 공격자가 검사하리라고 생각하는 하나의 포구를 감시함으로써(포구 19는 문자발생기인데 이것은 몇가지 취약점들을 가지고 있다.) 너무 많은 정보를 등록하는것과 수상한 자료흐름을 포착하는것사이의 균형을 깨뜨릴수 있다.

행 12와 13은 나가는 응답들을 Web와 우편봉사기만으로 제한하고 있다. 이것들은 봉사를 제공하는 유일한 두 체계이므로 인터네트호스트에로 응답을 보내야 하는 유일한 두개의 체계들이다. 행 14와 15는 UDP자료흐름을 DNS봉사기만으로 제한한다. UDP는 믿음성이 없으므로 안전하지 못하다. 이 려파기들은 취약점들을 하나의 체계에로 국한시킨다. 물론 이것은 모든 내부호스트들이 DNS변환을 위하여 우편체계를 리용하려고 할것이라는것을 의미한다.

행 16과 17은 하나의 호스트만이 경로기에로의 원격접속을 얻을수 있다는것을 규정하고 있다. 이것은 장치의 보호를 앞으로 더 강화하는데 도움이 된다. telnet를 리용하여 경로기를 관리할 때(경로기 대 경로기간의 암호화는 가능으로 하지 않고) 모든 정보는(통과암호를 포함하여) 평문으로 전송된다는것을 기억하시오. 이 려파기들은 어떤 사람이 통과암호들을 손상시킨다고 하여도 그것들이 하나의 원격체계에서 쓸모 있다는것을 담보한다(물론 공격자가 자기의 IP주소를 날조하고 우리가 거기에 가지 않는 한).

마지막으로 접근규칙들은 다음과 같은 말로 끝난다. 《우리가 명백히 거부하지 않은 TCP자료흐름은 내보내시오.》 만일 려파하려고 하는 TCP봉사들이 있다면 이 검사조건들을 이 마지막규칙의 앞에 넣어야 한다.

일러두기

변화된것들을 너무 인차 보관하지 말아야 한다. 동작중의 기억에서만 그 변화들의 검사를 진행하여야 한다. 만일 부주의로 장치를 잠그었다면 마지막에 보관된 구성에로 돌아 가기 위해 전원을 끌수밖에 없다. 새로운 구성에 대해서는 그 변화가 허용가능하다는것을 확인하고 보관하여야 한다.

동적접근목록

임의의 보안방책에도 례외가 있을수 있으며 동적접근목록은 바로 그 필요성의 반영이다. 이른바 《자물쇠-열쇠》라고도 부르는데 이 특징은 동적확장접근목록을 만든다. 그러나 그것은 표준 및 정적확장접근목록과 함께 리용될수도 있다.

자물쇠-열쇠가 기동되면 그것은 주어 진 대면부가 지정된 사용자에게 주어 진 자원에 접근을 허용하게 하도록 현존접근목록을 변화시킨다. 그리고 접근목록을 다시 변경시

켜 이전의 상태에로 복귀시킨다.

자물쇠-열쇠는 전통적인 표준 및 정적확장접근목록에 비하여 리익을 제공한다.

- 사용자는 질문구조를 통하여 인증된다.
- 큰 망에서 자물쇠-열쇠는 간단한 고리방법을 제공한다.
- 접근목록의 경로기처리는 감소된다.
- 경로기기반구조에서 보다 적은 열기가 진행된다.

자물쇠-열쇠가 어떻게 동작하는가를 다음의 실례로 본다.

1. 휴가중인 관리자가 원격으로 망에 련결하여 고장수리를 하여야 한다고 하자. 관리자는 경로기에 telnet대화를 연다.
2. 경로기는 사용자인증과정을 수행한다(그자체에 의하여 또는 TACACS+ 또는 RADIUS와 같은 개별적인 보안체계들을 통하여).
3. 인증이 성과적으로 되면 관리자는 telnet대화에 가입되고 경로기는 동적접근목록에 하나의 림시항목을 만든다.
4. 관리자는 지금 내부망에 접근권을 가지고 있으며 요구되는 변화를 첨가할수 있다.
5. 일단 끝나면 관리자는 하나의 새로운 telnet대화를 시작하고 수동으로 림시항목을 지운다. 관리자는 그 항목에 대하여 정지 또는 절대시간초과값을 지정할수 있다. 이 경우에 경로기는 자동적으로 시간완료후에 그 항목을 지운다.

실례로 다음의 코드를 고찰하자. 그것은 동적접근목록을 구성하기 위한 지령으로 시작된다.

```
access-list {access-list-number} dynamic {dynamic-name} {deny or
permit} telnet {source} {source-wildcard} {destination} {destination-
wildcard} precedence {precedence} tos {tos} established log
```

실천에서 관리방책은 수동으로 그 항목을 지우는것이지만 시간초과값설정은 잠재적인 보안구멍을 메우는 쉽게 구성가능한 보증방법이라고 말할수 있다.

속임수(spoofing)

자물쇠-열쇠에 의하여 만들어 진 동적접근목록의 림시항목은 그 경로기가 속임수를 겪게 만들수 있다. 이 위협에 대항하는 한가지 방법은 그 경로기와 원격호스트에 봉사하는 원격경로기에서 암호화를 사용하는것이다. 암호화된 련결을 가지면 호스트IP주소들은 잠재적인 해커로부터 암호화된 자료흐름속에 숨게 되며 따라서 속임수에 넘어 가지 않는다.

반사적접근목록

IOS 11.3부터 Cisco경로기들은 반사적접근목록을 지원한다. 반사적접근목록은 정적 establish지령을 위한 하나의 교체인것으로 만들어 졌다. 반사적접근목록이 리용될 때 경로기는 모든 동작중의 대화들에 대한 동적상태표를 만든다.

상태표를 만드는 능력으로 하여 Cisco경로기들은 실제적인 방화벽의 범주에로 접근하고 있다. 상태를 감시하는것에 의하여 경로기는 정적려과만을 지원하는 등가적인 장치들보다 려과결정을 하는데서 훨씬 더 좋은 위치에 있는것으로 된다.

반사적접근목록을 리용하기 위하여서는 대역식별자번호가 아니라 접근목록이름을 리용하여야 한다. 이것은 큰 일이 아니며 이름을 리용하는것은 보다 더 서술적이고 편리하다.

반사적접근목록을 만들기 위한 문법은 다음과 같다.

```
permit {protocol} {source} {mask} {destination} {mask} reflect
{name}
```

다음의 파라메터들을 리용하여 반사적접근목록을 만들수 있다.

```
permit ip any any reflect ipfilter
```

SMTP에서 하나의 내부호스트 그리고 내부망의 어떤 체계가 설정한 대화에 대한 응답들만을 허용하려고 한다고 가정하자. 이 환경에서 전체 구성방식에서 다음의것을 만들수 있다.

```
ip access-list extended inboundfilters
permit tcp any 206.121.73.21 0.0.0.0 eq 25
evaluate tcptraffic
```

이것은 동작중의 대화에로 들어 가는 응답들과 들어 가는 SMTP대화들이 설정되게 한다.

반사적접근목록과 관련한 한가지 제기되는것은 정지하여 300s후에 항목들이 표로부터 지워 진다는것이다. 이것은 대부분의 규약들에서 문제가 아니지만 FTP조종대화(포구 21)는 파일전송동안에 오랜 시간동안 정지되여 있을수 있다. 이 시간한계값을 다음의 지령으로 증가시킬수 있다.

```
ip reflexive-list timeout {timeout in seconds}
```

TCP차단

DoS(봉사거부)공격은 최근에 매우 류행되였다. 이 공격을 실현하는데 가장 널리 쓰

이는 방법은 SYN범람을 리용하는것이다. 공격자는 짧은 시간동안에 대량의 련결요청을 시작함으로써 SYN범람을 만든다. 련결요청들이 정당한 주소들로부터 오지 않기때문에 봉사기는 련결을 완성할수 없다. 그 결과로 봉사기는 틀린 요청들에 응답하려는 시도에 매여 달리게 되며 합법적인 봉사요청들(Web나 FTP, 전자우편과 같은)에 대답할 자원들을 남기지 않게 된다.

Cisco의 TCP차단장치는 모든 들어 오는 련결요청들에 대답함으로써 이 문제를 해결한다. 성공하면 그것은 그 봉사기와의 련결을 열고 두 련결을 실현한다. 만일 련결요청이 합법적인것이 아니라면 련결요청은 거절되고 하나의 턱값계수기가 증가된다. 이 계수기가 한계값에 도달하면 이 주소로부터의 모든 추가적인 련결요청들은 자동적으로 거절된다.

TCP차단을 기동하기

TCP차단이 가능으로 되기전에 확장접근목록을 만들어야 한다.

access-list {access-list-number} {deny or permit} tcp {destination}

다음에 TCP차단을 기동하는 지령을 입력한다.

ip tcp intercept list {access-list-number}

TCP차단은 두가지 방식으로 동작한다. 즉 차단 또는 피동적감시이다. 기정방식은 차단방식이다. TCP차단장치는 들어 오는 모든 SYN들을 중재하여 SYN-ACK로 응답한다. 원격호스트로부터 하나의 ACK를 받은후에만 경로기는 원래의 SYN요청을 봉사기로 통과시켜 3통로 TCP련결신호를 완성하게 한다.

마지막으로 경로기는 두 련결을 함께 결합시킨다. TCP차단이 피동감시방식으로 구성된다면 경로기는 련결요청에 일정한 시간동안(기정은 30s)에 응답이 있는 한 통신을 차단하지 않는다. 피동감시방식은 다음의 지령으로 구성된다.

ip tcp intercept mode {intercept or watch}

문맥에 기초한 접근조종

문맥에 기초한 접근조종(CBAC)은 OSI모형의 응용층에서의 정보를 리용하여 TCP 및 UDP망자료흐름을 려과하며 경로기의 량쪽에서의 자료흐름을 분석하고 허용한다. 응용자료를 볼수 있는 능력으로 하여 CBAC는 여러개의 통로들을 여는 규약들(RPC, FTP 그리고 대부분의 다매체규약들과 같은)과 Java애플리트(압축되지 않는 조건에서)를 위한 려과를 허용한다.

CBAC는 련결들을 동적으로 열기때문에(방화벽안쪽으로부터 시작된 대화들에 자료를 제한하면서) 그것은 DoS공격에 대한 방어를 제공한다. CBAC는 또한 TCP순서번호가 기대되는 범위안에 있는가를 확인하며 련결요청들이 비정상적으로 속도가 높아 지는것을 감시하고 응답한다.

응용프로그람에 기초한 등록과 경보는 CBAC의 또 한가지 우점이다. 시간도장, 원천 및 목적지주소들 그리고 전송된 자료들을 추적하는것에 의하여 CBAC는 해킹《징후》에 대하여 망패턴을 정합하는데 충분한 정보를 중앙집중적인 기록 및 관리체계에 넘

겨 주며 체계가 알려 진 침투 및 DoS방법들에 대한 방어를 일부 자동화할수 있게 한다.

CBAC는 일반적인 TCP 또는 UDP대화를 평가할수 있으며 또한 다음과 같은 널리 쓰이는 응용층규약들도 분석할수 있다.

- FTP
- TFTP
- H.323(Microsoft NetMeeting에 쓰는 규약)
- HTTP(Java애플리트 포함)
- Microsoft Netshow
- rexec, rsh, rlogin
- Real Media
- RTSP(실시간흐름규약)
- SMTP

CBAC실례

표본FTP대화를 리용하여 CBAC과정을 상세히 고찰하자.

1. 경로기의 외부대면부가 망의 내부(안전한)쪽에서 시작한 파케트를 받는다.
2. 경로기는 외부대면부에 정의된 나가는 접근목록을 리용하여 그 파케트가 허용될것인가를 결정한다. 허용되지 않는 파케트는 자동적으로 거절된다.
3. 만일 파케트가 허용된다면 CBAC는 하나의 새로운 련결상태표를 만들고 파케트의 정보를 거기에 넣는다.
4. 다음에 CBAC는 외부대면부에 들어 오는 접근목록을 림시로 변경시켜 내부망에로 들어 오는 대화자료를 허용한다(나가는 파케트로부터 취해 진것과 같은 상태자료와 련결상태표에 저장된것을 정합하는 파케트). 접근목록이 변경된후에야 CBAC는 외부대면부로부터 나가는 파케트를 전송한다.
5. 자료가 외부대면부로 돌아 올 때 모든 파케트들은 들어 오는 접근목록과 비교된다. 만일 정당한 련결자료가 CBAC에 의하여 접근조종목록에 만들어 진 림시변화와 정합된다면 이 파케트들은 내부망에 전송되고 련결은 끝난다.
6. 련결이 끝날 때(또는 시간초과된다면) CBAC는 련결상태표와 접근조종목록에서의 림시변화를 제거하고 경로기를 이전의 상태에로 귀환한다.

CBAC를 구성하기

CBAC를 구성하는데는 여러단계가 필요하다.

1. 대면부를 선택한다. DMZ(비무장지대)를 가진 망들에 대하여 내부대면부에 대한 평가가 진행된다. 간단한 망에 대하여서는 파케트들이 외부대면부에서 선별된다.
2. IP접근목록을 만든다. 하나의 기초적인 접근목록을 만든후에 모든 CBAC평가된 자료흐름은 허용되지만 모든 들어 오는 CBAC자료흐름은 거부된다 (CBAC는 이 규칙들에 자기의 동적 및 림시적례외들을 만든다.).

3. 시간한계와 턱값들을 설정한다. 이 설정들은 련결상태표가 얼마나 오래 유지되며 불완전한 련결이 끝날 때까지 얼마나 오래 기다릴것인가를 결정한다. 이것은 DoS공격에 대한 방어를 제공한다. 이 마지막 특징을 기동시키기 위해서는 조종탁에서 다음의 지령을 입력시킨다.

ip inspect tcp synwait-time {second}

4. 검사규칙을 만든다. 이것은 어떤 응용층규약이 대면부에서 평가될것인가를 결정한다. 선택가능으로는 경보, 조사 그리고 규칙이 IP토막화를 검사하는가 하는것이 있다. 이 실레는 하나의 FTP검사규칙을 설정한다.

ip inspect name ftprule ftp alert on audit-trail on timeout 30

5. 검사규칙을 적용한다. 이 규칙은 나가는 자료흐름이 외부대면부에 설정되였다면 그것에 적용되고 들어 오는 자료흐름이 내부대면부에 설정되였다면 그것에 적용된다. 우리의 실레를 계속하면

ip inspect ftprule out

6. 등록을 설정한다. 이것은 권한 없는 접근시도들을 결정하며 또한 합법적인 자료흐름과 봉사들에 대한 기록을 만든다. 전체 대역조사는 다음과 같은 기능으로 된다.

ip inspect audit-trail

방화벽침입검출체계

Cisco의 침입검출체계(IDS)는 59개의 공격징후들을 리용하여 해킹시도들을 인식하고 반응한다. IDS는 침해가 발생하기전에 공격을 인식하고 기록하며 반응하도록 설계되였다. IDS징후를 두 류형으로 갈라 볼수 있다. 즉 정보와 공격이다.

정보징후는 망에 대하여 정보를 수집하려는 시도들(포구주사와 같은)을 찾는다. 이 두 류형들의 매개는 또 원자징후와 합성징후로 갈라 진다. 원자징후는 특정의 포구에 대한 요청과 같은 작고 세부적인것들을 찾는다. 합성징후는 전체적인 패턴을 찾는다.

IDS과정

IDS체계는 다음과 같이 동작한다.

조사규칙을 만든다 임의의 수의 징후(하나로부터 모두)들이 하나의 규칙과 관련된다.

조사규칙이 적용된다 규칙이 들어 오는 자료흐름에 적용될 때 IDS는 ACL이 하기전에 그것들을 평가할 기회를 가지며 그것에 의하여 보통의 ACL거부에 의해서는 제거되지 않는 공격의 세부들을 제공한다.

파케트들을 검사한다 여러 모듈들이 파케트를 분석하는데 IP로부터 시작하여

ICMP, TCP 또는 UDP에로 옮겨 가서 응용층에서 끝난다.

징후를 맞추어 본다 하나의 파케트가 그 모형의 어느 부분에서 한 징후와 일치한다면 그것에 대하여 다음의 적당한 작용이 가해 진다.

- 경보: 중앙감시체계에 경보를 보낸다.
- 제거: 그 파케트는 전송되지 않는다.
- 재설정: 그 파케트의 재설정기발을 설정한다. 이 파케트는 다음에 그 련결의 매측에 보낸다.

IDS를 구성하기

IDS를 구성하기 위한 절차는 다음과 같다.

- IDS를 기동한다.
- 우편국을 기동한다.
- 조사규칙을 만들고 기동한다.

IDS를 기동하기 IDS를 기동하려면 전체 구성방식의 조종탁에서 두개의 지령을 입력하여야 한다.

첫번째 지령은 검사를 설정한다.

```
ip audit {protocol} {signature} {options}
```

두번째 지령에서는 특정의 징후를 정합하는데서 몇개의 보관된 사건들을 IDS관리자(IDS를 위한 중앙경계감시체계)에게 보낼것인가 하는 한계를 설정한다.

```
ip audit po max-events {quantity of events}
```

우편국을 기동하기 우편국은 IDS중앙관리체계와 IDS호스트들(IDS특징을 가지고 구성된 경로기들)사이의 점대점련결을 만드는 Cisco의 전용규약이다. 경보들은 우편국을 따라 등록파일 또는 IDS관리자에게로 전송된다.

```
ip audit notify nr-director/log
```

모든 호스트들은 1과 65535사이의 한 번호를 배당 받는다(호스트식별자: Host−id). 관리자에게는 모든 IDS경로기들과 함께 1부터 65535사이의 공통적인 기관의 번호가 배당된다(기관식별자: org−id).

```
ip audit po local hostid {host-id} orgid {org-id}
```

관리자를 위한 우편국파라메터들이 설정되여야 하는데 그것들은 다음과 같다.

rmtaddress 관리자의 IP주소
localaddress 호스트대면부의 IP주소
port 기정값 45000, 이것은 관리자가 경보를 듣는 포구번호이다.
Preference 만일 관리자에로 가는 하나이상의 경로가 구성되여 있다면 이 수(1 또는 2)는 이 특정련결에 대한 우선권을 결정한다.

Timeout 우편국이 하나의 련결을 결정할 때까지의 시간한계(초단위로)
application 어떤 형식의 체계가 사건들을 조종하고 있는가(등록파일 또는 관리자)?

ip audit po remote hostid {host-id} orgid {org-id} rmtaddress {ipaddress} localaddress {ipaddress} port {port-number} preference {number} timeout {seconds} application {type}

검사규칙을 만들고 기동하기 첫 두 지령은 파케트들이 어떤 정보징후 또는 공격징후와 일치할 때 어떤 기정의 작용이 발생하는가를 결정한다(경보, 제거 또는 재설정).

ip audit info alarm/drop/reset
ip audit attack alarm/drop/reset

일단 기정의 작용이 규정되면 사용자가 제공한 검사이름(이것은 그 규칙에 징후들을 배당한후에 사용된다.)이 징후형식(정보 또는 공격), 표준ACL 그리고 작용(경보, 제거, 재설정)과 함께 특정의 규칙에 배당된다.

ip audit name {audit-name} info/attack list {standard ACL} action alarm/drop/reset

일단 정의되면 규칙은 방향(안으로 또는 밖으로)에 따라 대면부에 적용된다. 이 지령은 대면부방식에서 리용된다.

ip audit {audit-name} in/out

마지막으로 보호하려는 망의 IP주소가 구성된다(전체 구성방식에서).

ip audit po protected {ip address}

인증대리자

Cisco의 인증대리자는 보안방책을 사용자특징과 결합시켜 개인들이 어떻게 망자원에 접근할것인가를 조종할수 있게 한다. 사용자특징은 그가 자료전송에 적극적으로 종사하고 있을 때에만 RADIUS 또는 TACACS+ 봉사기로부터 온다. Cisco는 인증대리자를 NAT, CBAC, VPN 그리고 IPSec 와 같은 다른 보안봉사들과 통합하였는데 이렇게 함으로써 모든 접근조종방책들의 일치한 통합을 달성하고 있다.

인증대리자는 사용자의 HTTP요청을 가로 채는 방법으로 동작한다. 만일 사용자가 이미 인증되였다면 대리자는 그 파케트를 전송한다(그리고 같은 련결에서 오는 련속적인 파케트들도 통과시킨다.). 만일 인증대리자가 그것들이 권한이 없는것으로 결정한다면 그 경로기의 HTTP봉사기는 사용자에게 사용자이름과 통과암호를 요구한다. 만일 사용자가 다섯번 시도해도 정확한 정보를 제공하지 못한다면 대리자는 2min동안 응답을 멈춘다(가입거부).

인증대리자가 사용자가 정당한 사용자이름과 통과암호를 제공하였다고 결정하면 그

것은 AAA봉사기로부터 사용자특징을 얻는것으로 된다. 이 특징에 기초하여 인증대리자는 안쪽 및 바깥쪽 대면부의 ACL에 련결을 완성하는데 필요한 동적항목을 만든다. 만일 그 사용자가 시간한계안에서 그 련결을 계속 리용한다면 그에게 자격을 다시 입력하도록 요구하지 않는다. 인증대리자는 시간한계가 지난뒤에 동적ACL변화들을 제거한다.

인증대리자를 구성하기

인증대리자를 구성하는데는 3가지 단계가 필요하다.

- AAA를 구성
- HTTP봉사기를 구성
- 응용대리자를 구성

AAA를 구성하기 다음의 지령은 경로기에게 AAA를 가능하게 한다.

aaa new-model

다음의 두 지령은 가입등록(RADIUS 또는 TACACS+)에서 사용자에게 기정으로 어느 인증봉사가 제공되는가를 정의하여 그 봉사들을 허용한다.

```
aaa authentication login default RADIUS/TACACS+
aaa authentication auth−proxy default {1st method} {2nd method} …
```

RADIUS 또는 TACACS+를 지정하기 위하여 다음지령을 사용한다.

```
radius/tacacs−server server host {hostname}
```

경로기와 봉사기사이에 암호화와 인중을 위하여 리용되는 봉사열쇠를 지정하기 위하여서는 다음의 지령을 사용한다.

```
raduys/tacacs−server key{key}
```

마지막으로 ACL은 인증봉사기로부터 돌아 가는 자료흐름을 허용한다.

```
access−list {number of access list}
permit tcp host {source} eq {tacacs} host {destination}
```

HTTP봉사기를 구성하기 이 지령들은 전체 구성방식에서 넣는다. 첫번째 지령은 경로기에서 HTTP봉사기를 가능으로 한다.

```
ip http server
```

두번째 지령은 AAA를 인증방식으로 설정한다.

```
ip http authentication aaa
```

세번째와 마지막지령은 어느 접근목록이 HTTP봉사기에 속하는가를 규정한다.

```
ip http access-class {number of access list}
```

인증대리자를 구성하기 마지막으로 인증대리자자신이 구성된다. 첫 지령은 시간한계를 설정하고 그후에 인증대리자는 ACL에 대한 동적변화들(사용자인증항목들과 함께)을 제거한다.

```
ip auth−proxy auth−cache−time {minutes}
```

다음지령은 사실상 인증대리자규칙을 만들고 그것을 HTTP규약과 결합시킨다.

Ip auth-proxy name {rule name} http

마지막지령은 대면부방식에서 넣은것인데 그 규칙을 대면부와 결합시킴으로써 그것을 기동한다.

ip auth-proxy {rule name}

응용프로그람넘기기

Cisco는 포구 대 응용프로그람넘기기(PAM)를 리용하여 회사나 기간들이 비표준(비등록)TCP 및 UDP포구들에서의 CBAC려과방책들을 만들수 있게 한다. PAM은 이것을 응용프로그람을 특정포구와 련결시키는 하나의 표를 만드는 방법으로 실행한다. 표준 ACL들을 리용하여 PAM은 전체 부분망 또는 하나의 호스트에 적용될수 있다. PAM표의 항목들에는 3가지 형태가 있다.

체계정의 이 항목들은 편집하거나 지울수 없으며 등록된(또는 잘 알려 진) 포구 대 응용프로그람넘기기들(TCP 21=FTP와 같은)로 이루어 진다.

사용자정의 이것은 포구 대 응용프로그람넘기기의 고객항목들인데 응용프로그람이 잘 알려 진 포구에 대응될수 없다는 제한성을 가진다(즉 HTTP는 TCP 21에 대응될수 없다. 이것은 이미 체계정의된 항목에 의하여 FTP에 지정되여 있다.).

호스트정의 이 선택항목은 IP호스트나 또는 부분망들에 대하여 넘기기가 명확히 만들어 지도록 한다. 이것은 내부부분망으로부터 Web봉사기의 고객(그러므로 숨은)포구에로 가는 HTTP자료흐름만을 허용하는것에 의하여 보충적인 보안을 만든다. 호스트정의항목은 체계정의넘기기를 무시할수 있는 유일한 방도이다.

PAM를 구성하기

PAM은 경로기에서 응용프로그람이름과 포구번호 그리고 PAM을 표준ACL과 결합하는 선택항목(부분망 또는 호스트에 하나의 넘기기를 적용하기 위하여)을 지정함으로써 가동으로 된다.

ip port-map {application name} port {port number} list {ACL number}

이전의 한가지 지령의 변종을 리용하여 넘기기를 지운다.

no ip port-map {application name} prot {port number} list {ACL number}

표준포구 대 응용프로그람넘기기를 무시하려면 두개의 지령이 필요한데 하나는 특정호스트에 적용되는 표준ACL을 만들고 하나는 포구넘기기무시를 만든다.

access-list {ACL number} permit {IP address of host}
ip port-map {application name} port {port number} list {ACL from access-list command}

망주소변환

망주소변환(NAT)은 원래 IP주소들을 보존하기 위한 기술로서 착상한것인데 인터네트로부터 망IP주소들을 숨김으로써 망보안의 보충적인 층을 제공한다. NAT는 기관들이 사설IP주소대역을 리용하면서 인터네트와의 련결도 가질수 있게 해준다.

Cisco는 다음의 술어들을 리용하여 NAT개념들을 리해하게 하고 구성이 명백해 지도록 하고 있다.

내부국부주소 내부망의 호스트에 배당된 사설IP주소

내부전역주소 내부국부주소(사설망의 호스트에 지정된)로부터 나가는 자료에 그것이 NAT경로기를 통과할 때 배당되는 공개IP주소

외부전역주소 호스트의 소유자에 의하여 배당되는 호스트IP주소(그리고 정당한 공개인터네트주소)

외부국부주소 바깥망의 호스트가 내부망에 나타날 때의 IP주소. 외부전역주소는 내부사설망에 숨겨 질수도 있다.

NAT를 수행하는 경로기는 기관의 사설망과 공개인터네트사이의 경계에서 동작한다. 내부망의 한 호스트가 외부전역주소를 가지는 한 호스트(공개Web봉사기와 같은)에 련결을 요청할 때 그것은 NAT경로기에로 그 파케트를 보낸다. NAT는 그 파케트의 원천IP주소(그 호스트의 내부국부주소)를 어떤 외부전역주소(인터네트에 련결된 NAT호스트)에 전송한다. 인터네트호스트가 그 파케트를 돌려 보낼 때 그것은 자기의 외부전역주소를 원천주소로 지정한다. 그 파케트가 NAT에 도착하면 NAT는 목적지외부전역주소를 해당 호스트의 내부국부주소로 바꾸고 그것을 내부호스트에 전송한다. NAT는 이 과정을 그 대화기간 반복한다.

정적주소변환

NAT는 정적 및 동적주소변환을 수행할수 있다. 정적변환은 하나의 내부국부주소를 하나의 내부전역주소와 련관시킨다(이것은 내부망에서 나가는 어떤 다른 대화들과 공유되지 않는다.). 정적변환은 외부전역주소가 내부망의 한 호스트와 통신대화를 시작할수 있게 하며 지정된 내부국부주소는 비밀로 유지한다. 실례로 내부망에 위치한 하나의 Web봉사기를 가지고 있는데 아직 외부전역주소에서 시작되는 HTTP대화를 받아야 할 때 정적주소변환을 리용한다.

정적주소변환을 구성하는 첫 단계는 내부국부주소를 내부전역주소와 련관시키는것이다.

```
ip nat inside source static
```

마지막 4개의 지령은 NAT와의 관계에서 내부 또는 외부에서의 사설 및 공개대면부들을 정의한다.

```
interface {type} {number}
ip nat inside
interface {type} {number}
ip nat outside
```

동적주소변환

동적주소변환은 내부국부주소를 주소들의 어떤 저장소로부터 선택된 내부전역주소와 결합시킨다. 이것은 인터네트봉사를 위한 의뢰기로서 동작하는 내부망의 호스트에 대하여 가장 공통적인 구성이다. 이것은 또한 관리부담이 가장 적다.

동적주소변환을 가능하게 하기 위한 처음 지령은 IP주소들의 한 대역을 만든다(주소저장소).

ip nat pool {name of pool} {starting IP address} {ending IP address}

다음에 어느 내부국부주소가 변환되게 되는가를 정의하는 하나의 ACL이 만들어진다.

access list {access list number} permit {source}

동적주소변환은 이전의 지령에서 만들어 진 접근목록을 지정하여도 가능하다.

ip nat inside source list {access list number} pool {name of pool}

마지막 4개의 지령은 NAT에 관하여 내부 또는 외부의 사설 및 공개대면부들을 정의한다.

```
interface {type} {number}
ip nat inside
interface {type} {number}
ip nat ourside
```

사용자인증과 권한부여

Cisco경로기들은 망자원의 접근(경로기자체에로의 접근도 포함하여) 에서 사용자인증과 권한부여를 리용한다. 인증은 사용자의 신분을 확인하는 과정이다. 권한부여는 보통 인증의 바로 뒤에 오는것인데 사용자가 자원에 접근하는데 필요한 허가권을 가지고 있다는것을 확인한다. 두 경우에 개별적인 보안봉사들이 공통적으로 리용된다(RADIUS, Kerberos, TACACS와 TACACS+).

경로기에서 인증 및 권한부여봉사를 가능하게 하는데는 3가지 단계가 있다.

- AAA를 기동한다.
- 인증을 기동한다.
- 권한부여를 기동한다.

AAA를 기동하기

경로기에서 AAA를 기동하는것은 매우 간단하다. 그러나 TACACS와 TACACS+는 낡은 규약들이고 AAA와는 호환가능하지 않는다는것을 알아야 한다(AAA는 보다 새로운 RADIUS와 Kerberos규약들을 위하여 설계되였다.).

전체 구성방식에서 다음의 지령을 입력하시오.

```
aaa new-model
```

AAA를 끄는것은 그것을 기동하는것만큼 쉽다.

```
no aaa new-model
```

인증을 기동하기

인증(권한부여도 류사)은 하나의 방법목록에 의거하고 있다. 방법목록은 사용자가 경로기에서 인증(또는 권한부여)될수 있는 여러가지 방도들을 포함한다. 어떤 경우에 봉사들중 하나가 준비되여 있지 못할수 있는데(RADIUS봉사기가 정지되였을수 있다.) 경로기는 사용자를 인증하기 위하여 여별의 방법을 리용할수 있다(국부적으로 보관된 사용자자료기지 또는 또 하나의 RADIUS봉사기). 개별적인 인증자료를 정의할 대신에 방법목록은 집단으로 정의된다. 하나의 집단은 하나이상의 같은 형식의 봉사를 가질수 있다(즉 RADIUS집단에서 하나 또는 여러개의 RADIUS봉사).

첫 지령은 집단이름과 그 성원들의 IP주소들을 정의한다.

aaa group server radius {group name} server {ip address}

다음 지령은 《default》라는 제목을 가지는 하나의 방법목록을 정의하고 그것을 모든 경로기가입자들에게 적용한다. 모든 사용자들은 그 집단안의 모든 봉사기들이 도달불가능하지 않는 한 RADIUS집단에 의하여 인증된다. 도달불가능하면 경로기는 국부사용자자료기지를 찾아 본다.

aaa authentication login default group radius local

권한부여를 기동하기

방법목록은 어디서 체계가 사용자접근을 정의하는 체계분석표를 찾고 검색할것인가를 정의하는데도 리용된다. 권한부여방법목록은 인증방법목록과 류사한 방법으로 구성되는데 여러가지 방법에 의하여 어느 망봉사가 조종되는가를 정의한다. 이 망봉사들은 5개의 류형으로 볼수 있다.

Auth−proxy 방책들을 사용자에 결합시키는데 리용되는 인증대리자체계의 부분
Command 경로기에서 EXEC방식에서 주어 진 특성지령들에 대한 접근을 정의
EXEC 경로기말단대화의 특징을 일반적으로 규정
Network PPP를 포함하는 모든 망대화
Reserve Access 역telnet대화와 관련된다.

첫 지령은 방법목록을 만든다.

aaa authentication auth−proxy/network/exec/commands {level}/ {reverse−access {list name} {method}

두번째 지령(대면부방식에서 수행)은 권한부여방법목록을 대면부와 련결한다.

Login authorization {list name}

보충적인 보안예방책

지금까지 본 모든 보안예방대책들과 함께 목록에 첨가할만 한 가치가 있는것이 또 한가지 있다. 우리의 최종과제는 스머프(Smurf)공격을 막도록 하는것이다. 스머프라는 이름은 이 공격을 진행한 원래의 프로그람으로부터 붙은 이름인데 스머프는 하나의 호스트를 자료흐름으로 포화시켜 봉사거부를 일으키기 위하여 IP속임수와 ICMP응답들의 결

합을 리용한다.

이 공격은 다음과 같이 진행된다. 공격자는 가짜ping파케트(echo요청)를, 많은 수의 호스트들을 가지고 있으며 큰 대역너비의 인터네트련결을 가지는 망의 방송주소로 보낸다. 이런 망을 바운스싸이트라고 한다. 이 가짜ping파케트는 공격하려고 하는 체계의 원천주소를 가지고 있다.

이 공격의 전제는 경로기가 IP방송주소(206.121.73.255와 같은)로 전송된 하나의 파케트를 수신할 때 그것은 이것을 망방송으로 인식하고 그 주소를 이써네트방송주소 FF:FF:FF:FF:FF:FF로 넘긴다는것이다. 그러므로 경로기가 인터네트로부터 이 파케트를 수신하면 그것은 그것을 국부망토막의 모든 호스트들에 방송할것이다.

다음에 무슨 일이 생길것인가는 독자도 알리라고 본다. 그 토막의 모든 호스트들은 가짜IP주소에 echo응답으로 응답한다. 만일 이것이 큰 이써네트토막이라면 500개 또는 그 이상의 호스트들이 매 echo요청에 응답할수 있다.

대부분의 체계들은 ICMP자료를 될수록 빨리 처리하려고 하므로 공격자가 가장한 체계(목표체계)는 echo응답들에 의하여 인차 포화되게 된다. 이렇게 되면 체계는 다른 자료흐름을 처리할수 없게 되며 결국 봉사거부에 빠지고 만다.

이것은 목표체계에만 영향을 미치는것이 아니라 그 기관의 인터네트련결에도 영향을 미친다. 만일 바운스싸이트가 T3련결(45Mbps)를 가지고 있는데 목표체계의 기관은 임대선(56Mbps)에 련결되여 있다면 T3련결에로의 오고가는 모든 통신은 점차 마비되고 말것이다.

그러면 이러한 형태의 공격을 어떻게 하면 막을수 있겠는가? 스머프공격의 효과를 약화시키기 위하여서는 원천싸이트, 바운스싸이트 그리고 목표싸이트에서 다 대책을 세워야 한다.

원천에서 스머프를 막기

스머프는 가짜 원천주소를 가지고 echo요청을 전송하는 공격자의 능력에 기초하고 있다. 이 장의 앞부분에서 고찰한 표준접근목록을 리용하여 이 공격을 그것의 원천에서 중지시킬수 있다. 이것은 자기의 망에서 시작하는 모든 자료흐름들이 적당한 원천주소를 가지도록 담보함으로써 그 원천으로부터 공격을 하지 못하게 한다.

바운스싸이트에서 스머프를 막기

바운스싸이트에서 스머프를 막는데는 두가지 선택이 있다. 첫째는 간단히 모든 들어오는 echo요청들을 막는것이다. 이것은 이 파케트들이 망에 도달하지 못하게 한다.

둘째로 만일 들어 오는(모든 echo요청들을 막는것이 선택이 아니라면) 자기의 경로기들이 국부망방송주소를 목적지로 하는 자료흐름들을 넘기지 않도록 하여야 한다. 이것을 막음으로써 체계는 이 echo요청들을 더는 수신하지 않게 될것이다.

Cisco경로기가 국부망방송파케트들을 막도록 하기 위하여서는 국부망대면부에 대한 구성방식에 들어 가서 다음의 지령을 입력하여야 한다.

no ip directed-broadcast

경 고

이것은 매 경로기의 매 국부망대면부에서 수행되여야 한다. 이 지령은 경계선경로기에서만 수행되면 효과가 없을것이다.

목표싸이트에서 스머프를 막기

ISP의 도움을 받을수 없을 때에도 자기의 WAN련결에 주는 스머프의 영향을 막기 위하여 무엇인가 좀 할수 있다.

이 자료흐름들을 망경계선에서 막을수 있는데 이것은 이 공격이 그 망의 WAN대역너비를 몽땅 먹어 치우지 못하게 하기에는 너무 늦다.

그러나 경계선에서 그것을 막음으로써 적어도 스머프의 효과를 최소화할수 있다. 재귀접근목록 또는 상태를 유지할수 있는 어떤 다른 방화벽장치를 리용함으로써 이 파케트들이 들어 오지 못하게 할수 있다. 상태표는 공격대화가 국부망에서 시작되지 않았다는 것을 알고 있으므로(그것은 원래의 echo요청을 보여 주는 표항목을 가지고 있지 않다.) 이 공격은 처리될수 있으며 즉시 제거된다.

요 약

이제는 Cisco경로기에서 기초적인 련결을 어떻게 구성할것인가를 잘 알게 되였다. 우리는 자료흐름을 조종하기 위하여 표준 및 확장접근목록을 어떻게 만들것인가를 고찰하였다. 대부분의 망경계선들에 경로기가 있으므로 이 지식은 매우 쓸모 있을것이라고 본다. 려과를 어떻게 구성할것인가를 알게 되면 이 점에서 자료흐름을 조종할수 있게 된다.

보다 높은 준위의 보호가 필요하다면 완전특징을 갖춘 방화벽을 리용하여야 한다. 다음장에서는 Check Point의 방화벽-1을 어떻게 설치하고 구성할것인가를 고찰하게 된다.

제7장. Check Point의 방화벽-1

이 장에서 어느 방화벽을 취급할것인가를 선택하기는 좀 어렵다. 시장에는 넓은 범위의 특징들을 가진 많은 방화벽제품들이 나오고 있다. 방화벽-1은 현재까지 가장 널리 보급된것이기때문에 그것을 선택하여 고찰하기로 한다. 그것은 제6장에서 본 Cisco경로기를 제외하고는 다른 어느 방화벽제품들보다 많이 배비되였다.

방화벽-1의 개괄

방화벽-1은 넓은 범위의 특징들을 가지고 있지만 보안방책들을 만들고 집행하는데서 세가지의 기본구성요소들을 리용한다.

- GUI관리대면부
- 관리봉사기
- 방화벽모듈

GUI관리대면부

하나의 GUI의뢰기가 리용되여 망(또는 기업소)보안방책(주소변환 및 대역너비방책과 함께)을 정의하는데 이것은 또한 망객체(호스트들, 관문들 등)들과 보안규칙들에 의하여 정의된다. GUI는 등록보기(Log Viewer)와 체계상태보기(System State Viewer)를 가지고 있다.

방화벽-1은 GUI에서 정의된 방책들(보안, 주소변환 및 대역너비)로부터 INSPECT스크립트를 만든다. INSPECT는 Check Point의 전용의 객체지향적인 고급스크립트언어이다. INSPECT스크립트는 콤파일되여 INSPECT코드를 만드는데 이것은 다음에 망에 있는 여러가지 검열(Inspection)모듈들에 적재된다.

원래의 INSPECT스크립트는 본문파일이므로 그것들은 구체적인 요구들에 맞추기 위하여 보안관리자들에 의하여 변경될수 있다.

관리봉사기

GUI의뢰기를 리용하여 여러가지 방책들을 만드는데 그것들은 관리봉사기에 보관된다. 관리봉사기는 모든 방화벽-1의 자료기지들(망객체와 사용자정의를 위한것들을 포함하여), 방책들 그리고 모든 망집행점들에 대한 등록파일들을 보관유지할 책임을 진다.

방화벽모듈

방화벽모듈은 망집행점(보통 관문)에 설치되는 쏘프트웨어요소이다. 방화벽모듈은 관리봉사기로부터 방책들을 받아서 그것을 실현하며 그것에 의하여 망을 안전하게 한다.

검열모듈

검열모듈은 OS에서 적재되는데 망층아래(OSI모형에 기준하여 아래), 그러나 자료련결층우에 적재된다. 파케트들은 검열모듈에 의하여 분석되고 방책들과 비교된다.

이전의 통신들로부터의 IP주소들, 포구번호들 그리고 상태정보들이 모두 검열모듈에서 분석되여 방책이 그 파케트들을 허용하는가를 결정한다. 모든 대화들에 대한 모든 문맥과 상태정보들은 동적련결표에 보관된다. 이 표들은 부단히 갱신되는데 검열모듈에 다음의 통신들을 검사하는데 쓸 루적자료들을 제공한다.

보안봉사기

보안봉사기들은 사용자인증과 내용보안의 책임을 진다. 인증은 FTP, HTTP, Rlogin 그리고 telnet들을 가지고 동작할수 있다. 방화벽-1에서 리용될수 있는 인증체계(또는 제작자의 기술들)들의 일부를 들면 다음과 같다.

- 방화벽-1의 통과암호
- OS통과암호
- S/Key
- SecurID Token
- RADIUS
- Agent Pathways Defender
- TACACS/TACACS+
- 수자식증명서(Digital Certificates)

우의 체계들에서 리용될수 있는 3가지 인증방법이 있다.

사용자인증 이것은 투명하게 수행되는데(사용자는 방화벽-1관문에 표면적으로 련결되지 않는다.) 사용자인증은 임의의 IP주소로부터의 접근을 허용한다.

의뢰기인증 의뢰기인증은 임의의 봉사에 대하여 준비되여 있는데 특정의 IP주소와 련결되며 투명할수도 있고 투명치 않을수도 있다.

대화인증 사용자련결요청은 방화벽-1에서 차단되는데 이것은 다음에 대화인증기구(의뢰기에 설치되여 있는)를 기동시킨다. 자격을 받게 되면 방화벽-1은 련결요청을 끌낸다.

보안봉사기들은 또한 내용보안의 책임도 가지는데 이것은 다음의 규약들에 대하여 준비되여 있다.

HTTP 체계(HTTP, FTP 등), 방법(GET와 POST), 호스트들(*.com), 경로들 그리고 질문들에 기초하여 내용을 조종한다.

FTP 파일에서 반비루스검사 그리고 파일이름제한, FTP지령들(GET와 PUT)에 기초하여 내용을 조종한다.

SMTP 주소마당(《From》과 《To》), 머리부 그리고 부속형태 (*.VBS)에 기초하여 내용을 조종한다. 주소변환도 준비되여 있으며 응답으로 정확한 주소를 재보관하는 능력을 유지하면서 실제사용자이름을 바깥세계로부터 숨긴다.

보안 및 관리봉사

인증과 내용려과에 추가하여 방화벽-1은 다음의 보안 및 관리봉사들을 제공한다.

- NAT(망주소변환)
- VPN(가상사설망)
- LDAP(가벼운 등록부접근조종)구좌관리
- 제3자의 장치관리(열린 보안확장)
- 고장극복성(높은 리용성)
- 부하균형(련결조종)

망주소변환(NAT)

NAT는 사설IP주소들을 하나 또는 몇개의 공개IP주소들로 넘긴다. 방화벽-1은 두가지 방법을 통하여 동적 및 정적주소넘기기를 제공한다.

도형주소변환규칙기지 주소변환규칙기지는 IP주소에 의해서가 아니라 이름에 의하여 객체를 규정하는데 리용될수 있다(이전에 하나의 IP주소를 배당 받았던 객체). 규칙들은 다음에 특정의 목적지와 원천IP주소 또는 봉사들에 적용될수 있다.

자동구성 자동구성에 의하여 변환특징들이 망객체들(망 또는 워크스테이션과 같은)에 배당되며 다음에 규칙들이 자동적으로 이 특징들에 대하여 생성된다.

가상사설망(VPN)

Check Point의 VPN-1관문은 방화벽-1과 선택적VPN모듈의 결합이다. VPN-1은 공업표준규약들을 지원하면서 싸이트 대 싸이트 및 원격사용자VPN접근을 제공한다.

- DES
- Triple DES
- IPSec/IKE
- 수자식증명서

VPN에 대하여 더 알고 싶으면 제10장을 보면 된다.

가벼운 등록부접근규약(LDAP)

방화벽-1은 구좌관리모듈을 리용하여 LDAP사용자들(그리고 봉사기들)은 어떤 다른 망객체와 같은 규칙들에 의하여 리용될수 있다. 한가지 간단한 실례는 관문뒤에 있는 자원에 접근을 요청하는 방화벽밖에 있는 사용자이다. 방화벽모듈은 제3자의 LDAP봉사기에 보관되여 있는 LDAP자료기지에 사용자가 제공한 자격을 확인할것을 물어 볼수 있으므로 큰 사용자자료기지를 준비할 필요는 없다.

구좌관리의뢰기는 방화벽-1 GUI로부터 또는 독립적인 응용프로그람으로부터 시작될수 있다. 많은 사용자들에게 구성정보를 한번에 적용하기 위하여 견본이 리용될수 있다. 견본에서의 어떤 변화는 그 견본과 관계되는 모든 사용자들에게도 자동적으로 전달된다. 포함되는 모든 요소들(방화벽-1, 구좌관리의뢰기, LDAP봉사기)이 SSL을 리용하므로 이 통신은 안전하다.

제3자의 장치관리

열린 보안확장(Open Security Extension)은 망확장방책을 3Com, Microsoft, Cisco 그리고 Nortel과 같은 제작자들로부터의 제3자의 보안장치들에 적용하는 선택적인 구성요소이다. 일단 보안방책이 결정되면 방화벽-1은 ACL(접근조종목록)을 만들고 그것을 망에 있는 매 경로기와 장치에 보낸다.

열린 보안확장은 또한 보안방책객체들, 등록통보문들과 같은 미리 존재하는 접근목록을 입구하는 능력을 가진다.

고장극복성

망우의 모든 방화벽모듈들은 련결 및 상태정보를 공유하므로 매 개별적인 방화벽모듈은 모든 망통신들을 완전히 알고 있다. 만일 하나의 방화벽모듈이 실패한다면 다른 방화벽모듈이 그것의 위치에서 조종을 넘겨 받고 련결을 유지한다.

매 련결의 상태표들은 방화벽모듈사이에서 부단히 동기화되므로 체계는 비대칭경로조종을 지원할수 있다. 이 정보가 없으면 같은 대화의 부분이지만 다른 경로와 다른 관문을 통하여 전송되는 파케트들은 다르게 해석될수 있으며 일부는 제거될수 있다.

부하균형

ConnectControl은 하나의 론리적봉사기객체(같은 봉사를 제공하는 여러개의 물리적봉사기들)를 만드는 선택적인 모듈이다. 특정봉사기의 모든 련결들을 주어진 하나의 론리적봉사기에로 안내하는 규칙을 정의할수 있다. 의뢰기들은 사실상 론리적봉사기를 구성

하는 물리적봉사기들중의 어느것에 련결되여 있지만 하나의 론리적봉사기만을 알면 된다.
다섯개의 부하균형알고리듬이 존재한다.

봉사기부하 봉사기에 부하측정체계가 설치되여 있을 때에만 쓸수 있다. 방화벽-1은 여러 체계들로부터 정보를 리용하여 어느 봉사기가 들어 오는 련결을 가장 잘 처리할수 있는가를 결정한다.

왕복(Round trip) PING자료가 어느 봉사기가 가장 짧은 왕복시간을 가지며 그러므로 하나의 련결을 처리하여야 한다는것을 결정한다.

회람(Round robin) 목록에 있는 다음번 봉사기에 련결이 배당된다.

우연(Random) 우연알고리듬에 의하여 하나의 봉사기가 선택된다.

령역(Domain) 령역이름에 의하여 결정했을 때 가장 가까운 봉사기가 선택된다.

좋은 방화벽-1의 지원을 찾기

Check Point밖에서 방화벽-1에 대한 가장 좋은 정보는 Phoneboy 특히 www.phoneboy.com에서 찾을수 있다. 이 싸이트는 가장 좋은 FAQ싸이트들중의 하나로서 다음의 주소에 방화벽-1을 전문취급한 목록을 가지고 있다.

www.phoneboy.com/fwl/wizards/index.html

물론 다음의 주소에 하나의 통보문을 보냄으로써 Check Point 방화벽-1우편목록에 예약할수도 있다.

<Majordamo @ us.checkpoint.com>

통보문은 다음과 같은 내용을 가지게 할수 있다.

Subscribe fw-1-mailing list

이 목록은 Check Point에 의하여 운영되고 있지만 사실 그리 적당한 목록은 아니다. 예약자들은 문제점들과 불만을 공개적으로 토론하고 있으며 Check Point로부터 그 목록에 정보를 올리는것을 거의 볼수 없다.

이것은 말단사용자공동체안의 친절한 사람들로부터 충고와 도움을 받고 있다는것을 의미한다. 이것은 언제나 좋은 일이다. 시장광고가 아니라 직접적인 조언을 더 많이 받게 되는것이다.

플래트홈의 선택

방화벽-1의 우점의 하나는 그것이 지원하는 플래트홈이 다양한것이다. 방화벽-1의 요소들은 표 7-1에서 보여 준것과 같은 여러가지 조작체계들에서 돌아 갈수 있다.

우리의 고찰을 위한 한가지 모형으로서 NT 4.0을 리용하기로 한다. 이 선택에는 다음의 몇가지 리유가 있다.

표 7-1 방화벽-1이 지원하는 조작체계

방화벽-1 모듈	조 작 체 계
관리봉사기와 집행모듈	Microsoft Windows NT 4.0 Sun Solaris 2.6, Solaris 7 Red Hat Linux 6.1 HP-UX 10.20, 11.0 IBM AIX 4.2.1, 4.3.2, 4.3.3
GUI의뢰기	Microsoft Windows 9×, NT, 2000 Sun Solaris SPARC HP-UX 10.20 IBM AIX

- 방화벽의 리용에서 UNIX체계를 안전하게 하는데 필요한 정보는 너무 널리 분포되여 있다. NT를 안전하게 하기 위한 기술들은 그리 공통적인것이 아니다.
- NT와 NT제품들은 UNIX제품들보다 그리 성숙되지 못하였고 따라서 설치과정에 감시하여야 할 많은 문제들을 가지고 있다.
- NT에서 방화벽을 돌리는것은 매우 인기 있는것으로 되고 있다.

이러한 리유로 하여 우리의 고찰은 NT판 제품들로 제한하려고 한다. NT와 UNIX판들사이에는 많은 대면부류사성들이 있지만(지어 UNIX우에서 방화벽을 돌리고 NT로부터 그 조종쏘프트를 돌릴수 있다.) 그 설치과정은 판들사이에서 크게 다를수 있다.

방화벽설치를 위한 NT준비

먼저 방화벽제품설치를 위하여 NT를 준비하는 과정을 보기로 하자. 보안을 강화하고 성능을 최량화하기 위하여 체계에 대한 수많은 작은 변경을 수행할수 있다.

하드웨어요구

방화벽으로서 리용될 제품NT봉사기는 다음의 규준들을 만족시키거나 초과하여야 한다(T1-속도의 련결 또는 그이하를 가지고 있고 봉사기는 방화벽기능으로 전용화되고 있다고 가정하고 있다.).

- Pentium 200처리기
- 1GB의 디스크기억
- RAID Ⅲ 또는 그이상의 여분
- 128MB의 RAM(Check Point의 권고에 따르면 방화벽-1을 위한 최소크기)
- 2개의 PCI망기판

방화벽-1은 보다 못한 플래트홈에서 돌것이므로 인터네트성능과 리용가능성이 중요

한 인자로 된다. 만일 처음으로 인터네트련결을 하고 있다면 다른 기업봉사들과 마찬가지로 얼마나 빨리 그것에 의존하게 되는가에 놀랄것이다.

NT의 설치

방화벽-1은 NT봉사기 또는 워크스테이션우에서 돌게 된다. 이 체계는 전적으로 방화벽기능만 하게 되여야 하므로 이 두 제품사이의 사용권계산차는 고려되지 말아야 한다. 그러므로 어느 한 제품을 리용할수 있다. 그러나 등록고(Registry)에서의 허용설정들에 의하여 NT봉사기가 좀 더 안전하게 되므로 NT봉사기를 리용하는것이 권고된다.

주 의

Windows NT 등록고(Registry)는 체계의 모든 구성정보를 보관하는데 NT봉사기와 워크스테이션사이에서 약간 다르다. NT봉사기는 등록고열쇠들에 관한 보다 엄격한 접근조종방책을 가지고 있다. 이것은 체계관리자만이 그 자료기지열쇠안에 보관된 값을 변화시킬수 있도록 담보하며 등록고정보의 무결성을 증가시킨다.

NT봉사기를 설치할 때 다음의 내용들을 관찰하여야 한다.

- NT를 적재하기전에 모든 필요한 망기판들을 설치한다.
- NT조작체계와 교체파일을 보관할 적어도 800MB의 NTFS C분할을 만든다.
- 나머지공간(최소 200MB)을 NTFS D분할로 만들어서 방화벽쏘프트와 방화벽등록파일(log)을 저장하는데 쓴다.
- 유일한 규약으로서 TCP/IP를 적재한다. IP전송이 가능한가를 확인한다.
- 이 봉사기를 내부접근을 위한 OS인증을 리용하는데 쓰려고 계획하지 않는 한 모든 봉사를 제거한다. 만일 OS인증을 리용하려고 한다면 콤퓨터열람기, NetBIOS대면부, RPC 구성봉사기 그리고 워크스테이션봉사들을 돌려야 한다.
- SNMP를 리용하려고 한다면 그것을 설치한다.
- 콤퓨터를 하나의 령역프레임으로가 아니라 독립적인 작업집단으로 구성한다.
- 만일 봉사기가 령역의 부분이라면 외부대면부에서의 모든 WINS결합을 불가능으로 한다.
- 손님구좌를 불가능으로 하고 방화벽관리를 위한 새로운 관리자등가구좌를 하나 만든다. 방화벽쏘프트를 설치할 준비가 되면 관리자로서의 가입을 제명하고 새로운 구좌이름으로 가입하며 관리자구좌를 불가능으로 한다.
- 사용자관리에서 검열과 가입실패추적을 가능으로 한다. 사용자권한에서 모든 사용자가 망으로부터 가입하는 권한을 지운다. 국부가입권한을 관리자등가로 만든 사용자이름만을 허용하도록 변경한다.
- Service Pack 6a를 설치한다. 이것은 가장 안정한 봉사묶음으로 인정되고 있으며 가장 포괄적인 보안요소들을 가지고 있다.
- 체계등록정보의 성능표쪽에서 우선권응용프로그람지원을 None으로 변경시킨다.
- 만일 봉사기봉사(령역인증을 위한)를 돌리고 있다면 봉사기등록정보대화칸에로 가서 망응용프로그람을 위한 처리량을 최대값으로 변경시킨다.

알려두기

NT는 구동기이름들을 등록고에서 NIC기판적재순서와 결합시키는 문제를 가지고 있다. 만일 기판설정이 어떤 방법으로(IRQ변화, 기판의 추가 또는 제거 등) 변화된다면 이 등록고설정이 혼란될수 있다. 이것을 ipconfig지령을 돌려 검사할수 있다. 이 지령은 부정확한 기판정보 또는 다음과 같은 오유통보문을 내게 한다. 《The Registry has become corrupt.》 그러므로 NT를 설치하기전에 NIC들을 설치하는것이 중요하다. 조작체계와 모든 수정쏘프트들을 재적재할수도 있다.

우의 내용들을 실행하였다면 이제는 구급회복디스크를 만들고 방화벽-1제품을 설치할 준비가 되였다. 만일 이제 NT봉사기 CD로부터 어떤 새로운 쏘프트를 적재한다면 다음의 내용들을 재설치하여야 한다.

- SP6a
- 모든 hotfix들
- 방화벽쏘프트웨어(갱신으로서)
- 방화벽수정프로그람(patch)
- 방화벽쏘프트웨어를 설치하기전에 체계가 정확히 당신이 원하는대로 되였는가를 확인하여야 한다.

설치하기전의 간단한 검사

이 점에서 그 방화벽플래트홈이 IP련결을 가지는가를 확인하여야 한다. 인터네트로 련결하는 국부경로기대면부에로 기정의 경로를 하나 만든다. 방화벽에 직접 련결되지 않은 어떤 내부망토막에 대하여 요구되는 경로표항목들을 만든다. 경로표항목을 만들 때 리용할 정확한 문법은 다음과 같다.

Route add-p {remote IP} mask {subnet mask} {gateway address}

국부경로기의 IP주소는 192.168.1.5이고 그 다른쪽에 있는 망 192.168.2.0에 가는 경로항목을 만들기 위해서 다음과 같이 입력한다.

Route add-p 192.168.2.0 mask 255.255.255.0 192.168.1.5

마찬가지로 경로기항목이 호스트 192.168.2.10에 대한것만이라면 다음과 같이 입력한다.

Route add-p 192.168.2.10 mask 255.255.255.255 192.168.1.5

주 의

-p표시는 조작체계로 하여금 이 경로항목을 영구적인것으로 만들도록 한다. 즉 조작체계가 재기동하여도 그 경로항목은 변하지 않고 남아 있도록 한다.

경로표를 만든 다음에는 련결성을 검사하여야 한다. 이것은 ping과 traceroute지령을 리용하여 할수 있다. 이 점에서 방화벽플래트홈은 모든 내부 및 외부호스트들과 련결을 가져야 한다. 만일 그렇지 않다면 앞으로 더 나가기에 앞서 그 문제를 해결하여야 한다.

또한 내부호스트로부터 외부IP주소에로 ping을 할수 있는가를 확인하여야 한다. 그러나 자기의 내부호스트들에 대하여 사설주소공간을 리용하고 있다면 이것은 불가능할 것이다. 사설주소공간을 리용하고 있다면 방화벽의 외부대면부에 ping을 하는것으로 충분하다.

또한 ipconfig지령을 돌려 외부IP주소와 관련된 적응기구동기이름을 기록하여야 한다. 하나의 관문장치를 구입하였다면 후에 방화벽쏘프트웨어설치시에 필요하게 될것이다. 그 항목은 매우 민감한것이므로 그 이름을 정확히 기록하였는가를 확인하여야 한다.

일러두기

만일 련결을 검사하는 동안 누가 망에 침입할가봐 걱정된다면 경로기의 WAN련결을 끊어 놓으면 된다. 그러면 그 경로기의 직렬대면부의 IP주소만큼은 멀리 련결을 검사할수 있다.

사용권받기

련결성을 다 검열하고 나면 방화벽사용권을 받을 준비가 된것으로 된다. 사용권을 받기 위하여 Web열람기로 다음의 위치를 지적한다.

http://license.checkpoint.com/

제시된 양식들에 내용을 써넣음으로써 그 제품을 등록하고 합법적인 사용권열쇠를 받을수 있다.

다음의 정보들을 써넣어야 한다.

- 당신은 누구인가?
- 당신의 전자우편주소
- 누가 당신에게 그 쏘프트웨어를 팔았는가?
- CD결봉안에 있는 증명서열쇠번호
- 당신이 리용하려고 하는 플래트홈과 조작체계
- 방화벽의 외부IP주소

이 양식을 완성하면 유효한 호스트ID, 특징모임 그리고 사용권열쇠를 받게 된다. 이 정보는 또한 그 양식에 써넣은 전자우편주소에도 보내진다. 일단 이 정보를 손에 넣으면 방화벽설치를 시작할 준비가 된것으로 볼수 있다.

주 의

방화벽쏘프트웨어는 지정된 날자에 만료되는 30일 평가판을 가지고 있다(그것이 설치돼서 30일이 아니다.). 필요하다면 이 사용권을 리용하여 방화벽을 다시 돌릴수 있으나 그 평가판은 요구하는 모든 선택안들을 다 지원하지는 않는다.

방화벽-1의 설치

방화벽-1 CD에는 모든 NOS판들을 위한 프로그람파일들과 사용지도서들의 Adobe Acrobat판들이 들어 있다. Windows등록부에서 방화벽봉사기쏘프트웨어들에 대한 등록부들과 많은 보충적인 요소들을 찾게 될것이다.

FloodGate-1 Check Point의 대역너비관리도구. 이 모듈은 특정한 형태의 망자료흐름에 대하여 대역너비를 담보하기 위하여 동작한다.

Meta IP 이 모듈은 사용자 대 주소넘기기를 하는것으로서 사용자에 기초한 보안방책들을 실현하고 등록하기 위하여 사용자신분을 IP주소와 자동적으로 련결하는 Check Point의 방법이다.

Reporting 미리 정의된 견본들을 제공하는것에 의하여 이 모듈은 Check Point 등록파일로부터의 정보를 정리하고 기록한다.

High Availability 이 모듈은 내용보안봉사를 위하여 봉사여분(하나의 봉사가 실패하면 다른것이 같은 과제수행을 인계 받는것)과 사슬련결(하나의 봉사는 실행가능성들을 검사하고 다음것은 권한 없는 ActiveX스크립트가 통과하지 않는가를 확인하는 등)을 제공한다.

VPN-1 SecuRemote Check Point의 VPN의뢰기이다. 이 쏘프트웨어는 의뢰기와 안전한 망사이의 모든 통신을 암호화한다.

VPN-1 Secure Client SecuRemote에 추가된것으로서 워크스테이션방화벽으로 기능한다.

Session Authentication Agent 이 요소는 Windows의뢰기가 방화벽-1모듈에 인증하고 어떤 허용된 IP봉사를 리용하도록 한다.

방화벽-1의 설치는 매우 간단하다. 먼저 CD를 NT봉사기에 설치한다(이것은 자동기동된다.). 다음에 사용권동의에 찬동하는가를 묻게 된다. 그러면 봉사기/관문요소 또는 이동용/탁상형요소를 선택하게 하는 제품안내서가 나타난다. 봉사기/관문을 선택한 다음 어느 특정의 봉사기/관문요소를 설치할것인가 하는 선택안이 나타나게 된다(기정은 그것들전체이다.).

다음에 독립형설치인가, 분산형설치인가를 결정하여야 한다. 마지막에 실제적인 방화벽-1설치가 시작되며 방화벽쏘프트를 어디에 설치할것인가를 묻게 된다. 관리가 쉽도록 하기 위하여 그 쏘프트웨어를 이전에 지정한 D분할에 설치하여야 한다. 다음에 그림 7-1에서 보여 준것처럼 어느 제품판본을 설치하려고 하는가를 선택한다. 대표적으로 이것은 방화벽-1 Enterprise Product(제한 없는 사용권 방화벽) 또는 방화벽-1 Single Gateway Product(250개까지의 호스트에 사용권허가되는 판본)일수 있다. 정확한 제품을 선택하는가를 확인하여야 한다. Single Gateway Product를 선택하면 후에 그 방화벽의 외부대면부를 식별할것을 요구하며 Enterprise 판에서는 그렇지 않다.

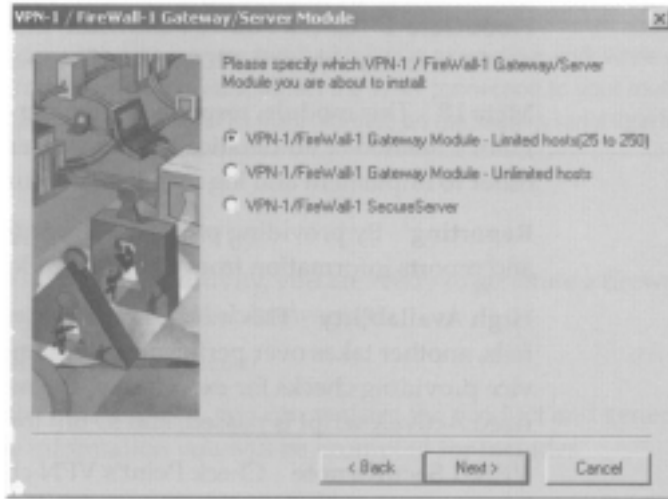



그림 7-1. 제품형선택대화칸

주 의

방화벽-1의 사용권은 병행가능한 인터네트련결의 수가 아니라 보호되는 마디점의 수에 기초하고 있다. 그 리유는 방화벽의 일이 IP호스트들을 보호하는것이기때문이다. 사용권이 방화벽뒤의 IP마디점들을 모두 포괄하는가를 확인해 보아야 한다.

적당한 제품을 선택하면 설치프로그람은 그림 7-2에서 보여 준것처럼 현재의 설치가 방화벽-1의 이전판본들과 호환되여야 하는가를 묻는다.

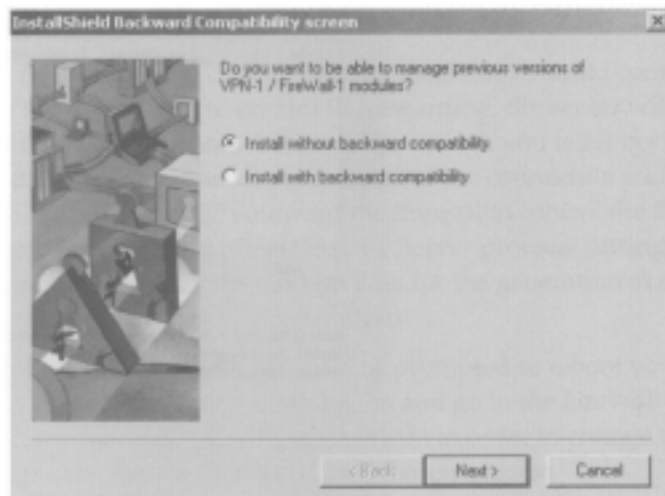



그림 7-2. 호환성화면

다음에 설치프로그람은 몇가지 추가적인 구성변화들을 수행하고 사용권정보를 입력할것을 요구한다. 만일 이 정보를 가지고 있다면 영구판을 설치하기전에 평가판을 제거

하는것이 좋다. 평가판은 사용권기간이 다 되면 사건보기에서 오유통보문을 낸다. 이것을 지우고 원하는것에로 다시 돌아 가야 한다. 그러므로 처음에 시작할 때 정확히 하는것이 더 쉽다.

다음에 그림 7-3에서 보여 준것처럼 방화벽관리자를 만들것인가를 묻는다. 방화벽관리자구좌정보는 Windows NT로부터 따로 보관된다. 관리자이름은 Windows NT에 접근할 때 리용하는 가입등록이름과 같지 않아도 된다.

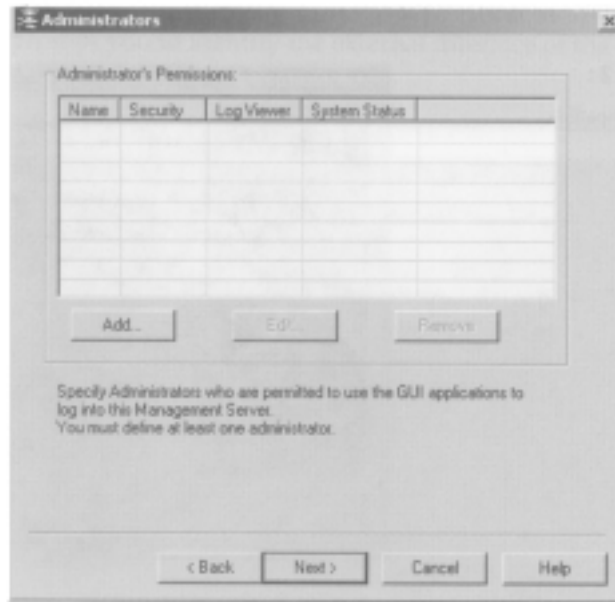



그림 7-3. 관리자대화칸

매 관리자에 대하여 허용되는 접근준위를 설정할수 있다. 다음과 같은 내용들을 선택할수 있다.

Read/Write All 사용자에게 모든 방화벽리용에 대한 완전한 접근이 허용된다. 이것은 보안방책들을 편집할수 있는 유일한 선택이다.

Customized Edit User와 System Status를 제외하고 다음의 모든 선택항목들을 읽거나 또는 읽기/쓰기 할수 있다.

- Edit User Database
- Security Rules
- Bandwidth Rules
- Compression Rules
- Log Viewer
- System Status

No Permissions 사용자는 허가객체를 가지지 못한다(그러나 기록의뢰기를 리용하는것은 허가될수 있다.).

Reporting Clients Permission 사용자가 기록도구와 등록파일정리프로그람을 돌리도록 허용하는가를 결정한다(또한 읽기만인가 또는 읽기/쓰기인가를 지정).

GUI의뢰기구성은 그 방화벽을 원격으로 관리하도록 허용되는 원격호스트들을 정의하게 한다. 원격사용자는 하나의 가입등록이름과 통과암호를 입력하여야 한다. 이 설정은 가입등록할수 있는 원천IP주소들의 수를 제한한다. 기정으로 관리는 방화벽자체에서만 허용된다.

전형적인 구성에서는 Monitor Only권한을 가지는 하나의 사용자를 만들고 GUI의뢰기설정을 리용하여 접근점들을 제한한다. 이 두 설정들을 결합하면 자기의 방화벽의 활동을 안전한 방법으로 원격에서 감시할수 있게 된다.

만일 하나의 관문을 설치하고 있다면 다음에 외부대면부를 위한 적응기의 이름을 입력하여야 한다. 이 정보는 지령창에서 ipconfig지령을 입력하여 검색할수 있다. 이 항목은 매우 민감한것이므로 문자렬을 정확히 입력하여야 한다.

다음에 방화벽-1이 IP전송을 조종할것인가를 선택하여야 한다. 만일 방화벽이 IP전송을 조종하게 하면 봉사기는 방화벽처리가 불가능으로 되므로 자료흐름을 통과시킬수 없게 된다. 또한 IP전송을 조종하지 않도록 하면 방화벽처리가 불가능으로 될 때 그 련결은 넓게 열려 져 있는것으로 된다.

명백히 보안을 강화하기 위하여 방화벽이 IP자료흐름을 조종하기를 원할것이다. 다음화면은 보안봉사기규약설정이며 다음 화면에서는 인증과 VPN운영에서 리용되는 암호화열쇠를 생성하기 위한 우연자료를 입력할것을 요구한다.

일단 설치가 끝나면 봉사기를 재기동하여야 한다. 봉사기가 다시 기동할 때 가입등록하고 방화벽-1프로그람묶음에로 가서 방화벽-1 구성그림기호를 선택하여 설치과정에 구성된 설정들의 일부를 변경시킬수 있다.

방화벽-1 GUI의뢰기의 설치

방화벽-1 GUI의뢰기는 CD에서 방화벽-1봉사기쏘프트와 같은 Windows등록부에 위치하고 있으며 기정에 의하여 방화벽-1 봉사기/관문모듈로 설치된다. GUI의뢰기는 4개의 분리된 요소들로 구성된다.

- 방화벽규칙들을 관리하기 위한 방책편집기
- 방화벽동작을 감시하기 위한 등록파일보기
- 개괄적인 자료흐름통계를 기록하며 방화벽이 정상인가 아닌가를 알기 위한 체계상태보기
- 사건이 발생할 때 그 통계를 보기 위한 실시간감시기

이 요소들은 방화벽자체가 설치되거나 또는 어떤 원격 Windows 9X 또는 NT/2000체계에 설치될수 있다. 또한 이 네개의 구성요소들의 매개를 선택적으로 설치할수 있다.

의뢰기요소들을 시작할 때 방화벽-1 가입등록화면이 나타날것이다. 방화벽-1 관리자로 만든 가입등록이름과 통과암호 그리고 방화벽봉사기의 호스트이름을 입력한다. 방화벽자체로부터 의뢰기를 돌리고 있을 때는 순환귀환주소(127.0.0.1)를 리용하기 바란다.

방화벽-1의 구성도구프로그람

지금 방화벽-1 쏘프트웨어가 설치되고 자기가 요구하는 어떤 관리자구좌를 첨가할수 있게 되였다. 방화벽-1 구성도구프로그람을 기동하고 관리자도구띠를 찰칵하면 그림 7-4의 화면이 나타난다.

그림 7-4에서 볼수 있는것처럼 이것의 선택항목들은 방화벽-1 봉사기설치기간에 관리자구좌를 만들 때의것과 같다.

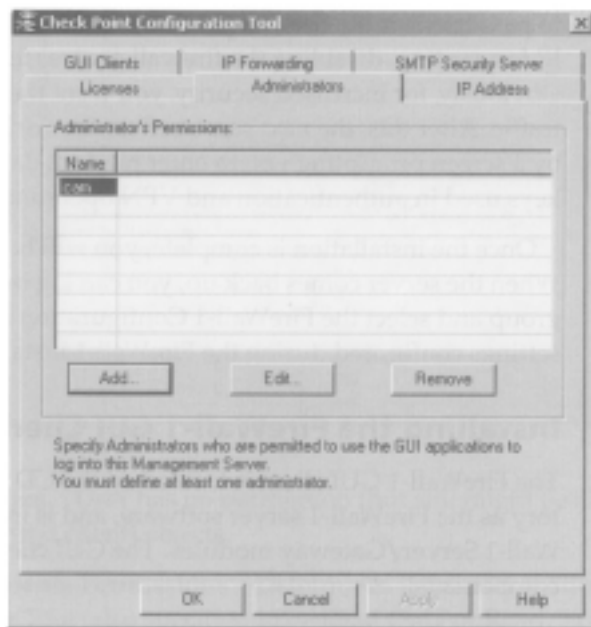



그림 7-4. 방화벽-1 구성도구의 관리자대화칸

방화벽-1 구성도구로부터 자기가 리용하려고 하는 SMTP보안봉사기도 구성할수 있다. 이것은 그림 7-5에서 보여 주고 있다.

SMTP보안봉사기는 방화벽-1 구성도구에 하나의 도구띠를 첨가하는 유일한 보안봉사기이다. 여기서 시간한계값, 우편통보문들을 보관하기 위해 어느 등록부를 쓸것인가, 오유통보문은 어디로 보낼것인가 등 SMTP과정을 위한 파라메터들을 정의할수 있다. NT는 내장된 우편기능을 가지고 있지 않으므로 오유통보문들은 체계의 이름과 적당한 우편구좌를 지정하여 원격의 우편체계에로 전송하여야 한다.

일단 구성을 완성하면 방화벽-1 구성도구프로그람을 닫을수 있다. 이제 방책편집기를 펼쳐서 방화벽규칙들을 만들수 있다.

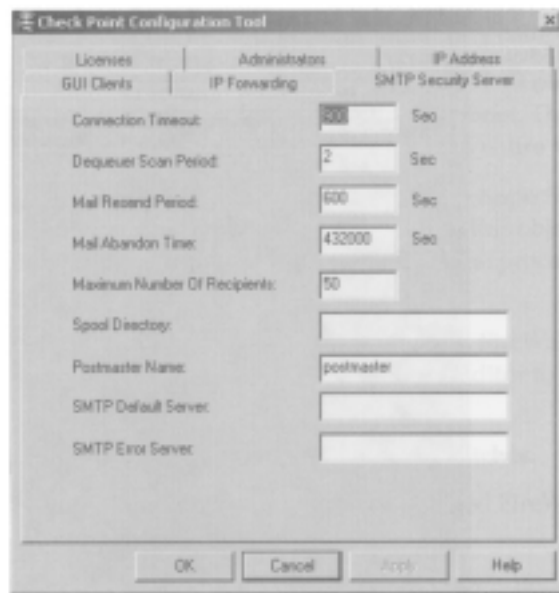



그림 7-5. SMTP보안봉사기

방화벽-1의 보안관리

방화벽-1을 통하여 보안방책을 관리하는것은 여러 단계의 과정을 걸친다. 처음에 조종하려고 하는 객체들을 정의하고 다음에 사용자들을 정의하며 그후에 이 객체들을

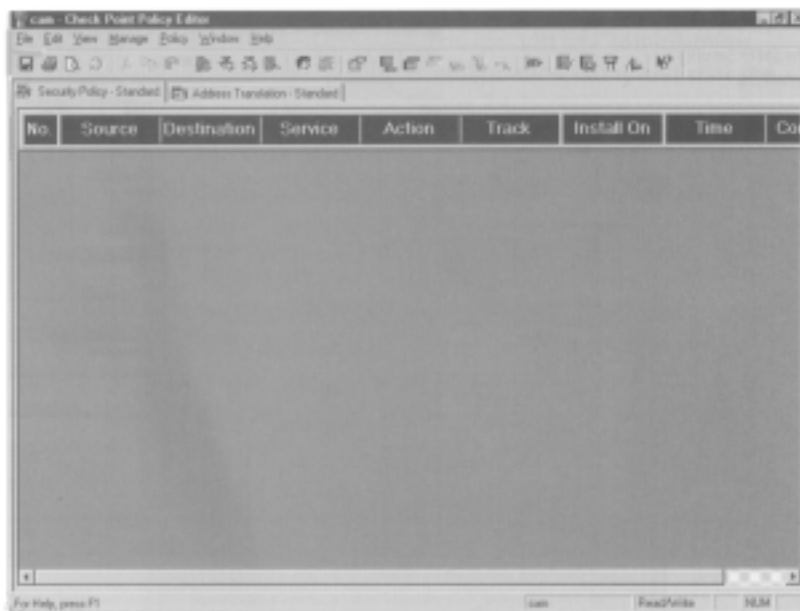



그림 7-6. 방화벽-1 방책편집기(Security Policy-1 화면)

규칙기지에 적용하여야 한다. 이 구성은 좀 복잡한것처럼 보일수 있지만 사실상 매우 직선적이며 매우 세밀한 보안조종을 할수 있게 한다. 모든 보안관리는 그림 7-6에서 보여준 방책편집기의 Security Policy-1을 통하여 수행된다.

이제 망객체들을 정의하는것으로부터 시작한다. Security Policy-1의 차림표로부터 Manage→Network Object를 선택한다(차림표선택항목들은 어느 방책표쪽(policy tab)이 선택되는가에 따라 변화된다.).

그러면 그림 7-7에 보여 준 Network Objects관리화면이 나타날것이다. 처음으로 이 화면을 시작할 때에는 항목이 없다.

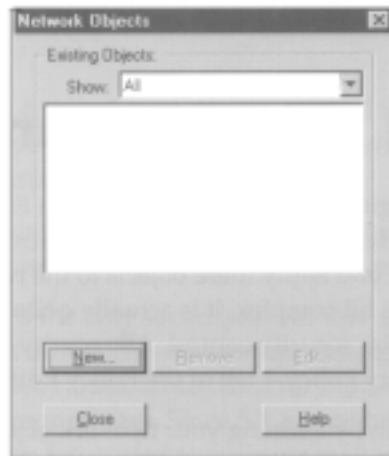



그림 7-7. Network Objects 관리화면

다음과 같은 각이한 형식의 객체들을 만들수 있다.

워크스테이션 이것은 콤퓨터호스트를 만드는데 리용되는 일반적인 객체이다. 이것은 방화벽과 같이 여러개의 NIC기판을 가지는 호스트들도 포함한다.

망 이 객체는 전체 IP부분망을 정의하는데 리용된다. 이것은 전체 부분망에 같은 보안방책을 적용하려고 할 때 유용하다.

령역 이 객체는 특정의 DNS령역이름안의 모든 호스트들을 정의하는데 리용된다. 이 객체는 리용하지 말것을 권고한다. 그것은 그것이 정확한 DNS정보에 의거하고 있고 방화벽의 처리속도를 느리게 하기때문이다.

경로기 이 객체는 망경로기들을 정의하는데 리용된다. 방화벽-1은 방책편집기에서 만든 방책들을 접근목록으로 변환하여 정의된 경로기들을 자동적으로 갱신하는 능력을 가진다.

교환기 이 객체는 망교환기들을 정의할수 있게 한다.

통합된 방화벽 이 객체는 설치된 방화벽모듈을 표현한다(집행점이라고도 부른다.).

집단 이 객체는 여러개의 객체들을 하나로 모으려고 할 때 필요하다. 실례로 모든 망객체들을 하나의 집단으로 만들고 그 집단을 local net라고 이름 붙일

수 있다.

론리봉사기 두개 또는 그이상의 모듈들을 집단으로 하여 같은 봉사를 제공할수 있게 하며 또한 부하균형을 가능하게 하는데도 리용된다.

주소대역 전체적인 IP부분망대신에 이 객체는 보안방책이 주소들의 모임에 적용될수 있게 한다.

방화벽을 위한 객체만들기

만들어야 할 첫번째 객체는 그 방화벽을 표현하는것이다. 이것은 Network Objects관리화면에서 New→Workstation을 선택함으로써 수행된다. 그러면 그림 7-8에서 보여 준 Workstation Properties화면이 나타날것이다.

먼저 하나의 이름과 IP주소를 배당한다. 체계이름은 콤퓨터의 DNS호스트이름과 Microsoft콤퓨터이름과 같아야 한다. 그리고 방화벽에 주목할 때 그것이 여러개의 대면부를 가지고 있지만 하나의 주소로 표준화하는것이 유리하다. 보통은 외부대면부가 리용된다. 이것은 국부DNS와 일치하여야 한다. 체계의 이름과 외부IP주소를 가지고 있는 방화벽에 하나의 hosts파일항목을 만들려고 할수도 있다.

일러두기

NT 봉사기가 C:/winnt/System32/drivers/etc 에 보관되여 있는 국부 hosts 파일에 자기자신을 위한 하나의 항목을 가지고 있다면 방화벽-1은 더 빨리 돌수 있다.

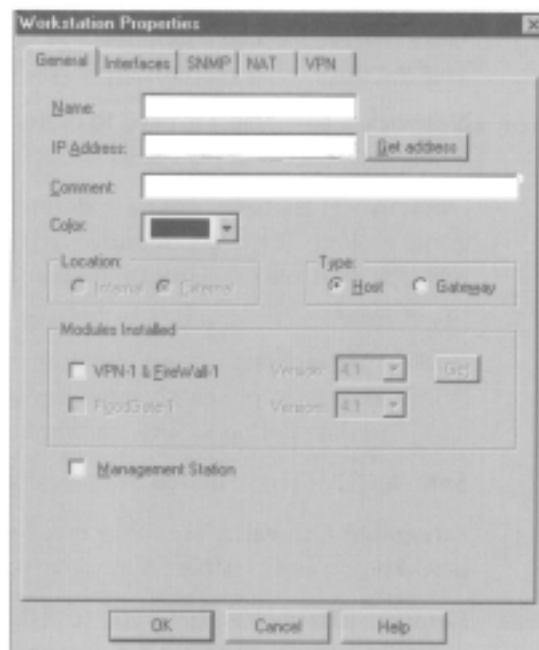



그림 7-8. Workstation Properties 화면

방화벽과 그뒤에 있는 체계는 내부망에 있는것으로 간주된다. 외부에 있는것으로 간주되는 유일한 체계는 방화벽의 외부대면부밖에 있는것이다. 그리고 이 체계는 여러개의 NIC기판을 가지고 있으므로 호스트가 아니라 관문으로 간주된다. 마지막으로 방화벽-1이 이 기계우에 설치되였다는것을 지적하여야 한다.

만일 Interface표쪽을 찰칵한다면 체계대면부들의 목록이 나타날것이다. 아직 어떠한 항목도 만들지 않았기때문에 이 목록은 비여 있을것이다.

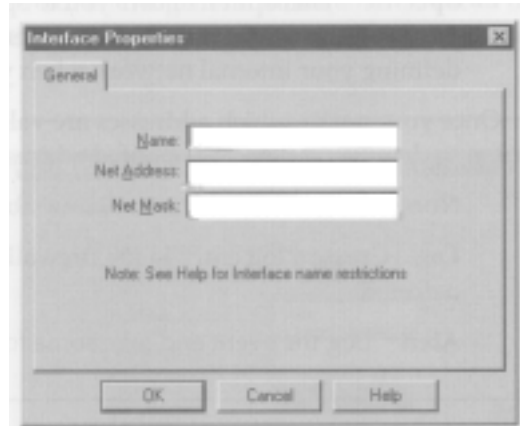



그림 7-9. Interface Properties화면

하나의 항목을 만들기 위하여서는 Add단추를 찰칵한다. 그러면 그림 7-9에 보여 준 Interface Properties 화면이 나타난다.

여기서 자기의 IP규칙들을 정의할수 있다. 자기의 매 대면부들을 구성함으로써 방화벽이 정당한 IP주소로부터의 자료흐름만을 허용한다는것을 담보할수 있다. 이것은 스머프와 가짜주소들을 리용하는 다른 공격들을 막는데 도움이 될것이다.

매 대면부에 대하여 리용하는 이름은 Windows NT에 의하여 리용되는 적응기이름과 같아야 한다. 이것은 IP속임수에 관한 규칙들이 정당한 대면부에 적용되도록 담보한다. 또한 국부적으로 부속된 망주소(NIC의 IP주소가 아니라 망의 부분망주소)와 적당한 부분망마스크를 입력하여야 한다.

다음에 어떤 자료흐름원천주소가 정당한가를 정의한다. 이것을 하기 위하여 Valid Addresses에서 선택항목들중 하나를 선택하여야 한다. 아래에서 매개 선택항목이 무엇을 의미하는가를 보여 준다.

Any 이것은 기정으로 되여 있는것인데 모든것이 잘 되여가고 있고 누구나 다 믿고 있다고 가정한다. 어떤 위장된 IP자료흐름에 대해서도 조사가 진행되지 않는다.

No Security Policy! 이것은 Any와 같다. 속임수검출이 진행되지 않는다.

Others 이 항목은 다른 대면부들에 대하여 정의된 속임수려파기와 결합하여 리용된다. 결과적으로 이 항목들은 다음의 내용을 서술한다. 《다른 대면부에서 정의된것을 제외하고 모든 자료흐름은 허용가능하다.》 이것은 외부

대면부에 대하여 보통 선택하는 항목이다.

Others+ 이것은 Others와 기본적으로 같은데 그것의 자료흐름이 허용가능한것으로 간주될수 있는 추가적인 호스트, 망 또는 집단을 정의하는 선택항목을 가지고 있다는것이 다르다.

This net 이 항목은 국부적으로 련결된 부분망으로부터의 자료흐름만이 허용된다는것을 지적한다. 이것은 DMZ 또는 다른 부분망에로의 경로련결을 가지지 않는 내부망토막을 정의하는데서 유용하다.

Specific 자료흐름이 허용가능한것으로 간주되는 특정의 호스트, 망 또는 집단을 지정할수 있게 한다. 이것은 여러개의 부분망을 가지고 있을 때 내부망을 정의하는데서 유용하다.

일단 어느 주소들이 정당한가를 규정하였다면 다음에 방화벽에 가짜주소가 검출될 때 무엇을 할것인가를 알려 주어야 한다. 다음의 선택항목들이 있다.

None 내가 가짜파케트에 대하여 무엇을 알려고 하는가?

Log 방화벽등록파일에 가짜파케트가 검출되였다는것을 지적하는 하나의 등록항목을 만든다.

Alert 그 사건을 등록하고 어떤 형태의 미리 구성된 작용을 한다.

주 의

Security Policy-1 차림표에서 Policy→Properties를 선택하고 Log와 Alert표쪽을 찰칵함으로써 Alert를 구성할수 있다.

최소로 망에 대하여 속임수파케트를 리용하려는 어떤 시도도 등록하여야 한다. Alert항목은 주의를 보다 빨리 끌게 할수 있는 어떤 다른 알림방법을 정의할수 있게 하므로 매우 유용하다. 실례로 방화벽이 경고조건이 성립된다는 내용을 가지는 하나의 전자우편통보문을 보내도록 할수 있다.

이 과정을 방화벽에 설치된 매 대면부에 대하여 반복한다. 그렇게 다 하였다면 OK를 눌러 방화벽망객체들을 보관할수 있다.

NAT작업

망객체들을 몇개 더 만들기로 하자. 내부망이 사설주소공간을 리용하고 있다고 가정하겠다. 이것은 방화벽이 내부망과 인터네트사이에서 망주소변환을 하여야 한다는것을 의미한다.

한가지 실례로서 우편중계기로 동작할 한 내부호스트를 설치하자. 이 호스트는 인터네트로부터 도달가능하여야 하므로 정적NAT를 리용하여야 할것이다. 방화벽객체들을 구성하는데 리용한 초기단계들을 반복한다. 구성에서 유일한 차이는 Workstation Properties화면의 General표쪽이다. 여기서 방화벽설치검사가 검사안된것으로 남아 있다. 서로 다른 객체들을 구별하기 위하여 이 객체에 대해서는 다른 색갈을 설정하려고 할수도 있다.

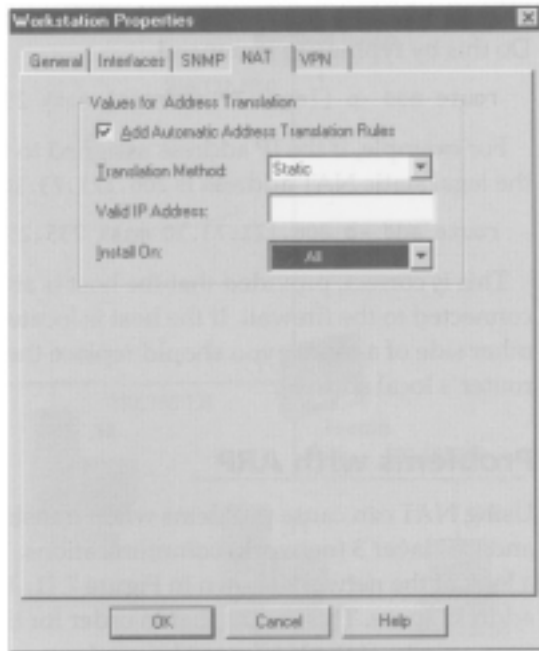



그림 7-10. Workstation Properties화면의 Address Translation표쪽

일반정보들을 다 채워 넣은 다음에 Interface표쪽을 선택하는것이 아니라 Address Translation표쪽을 선택한다. 이 화면은 그림 7-10과 류사하게 나타날것이다.

NAT를 리용하여 워크스테이션객체를 구성하는것은 매우 직선적이다. Add Automatic Address Translation Rules 검사칸을 선택하면 다른 선택항목들이 능동상태로 된다. 변환방법에 대하여 다음의 두가지중 하나를 선택할수 있다.

Hide 그 체계를 합법적인 주소뒤에 숨긴다.
Static 이 사설주소를 합법적인 주소로 넘긴다.

이 체계는 도달가능하여야 하므로 변환방법은 Static로 정의한다. 다음에 Valid IP Address마당에서 리용하려는 하나의 합법적인 IP주소를 입력한다. Install On선택항목은 어느 방화벽객체가 주소변환규칙을 집행하는가를 선택하게 한다. All을 선택하면 모든 방화벽객체들에 규칙들을 설치한다. 마지막으로 OK를 찰칵하고 규칙기지에 이 항목을 설치한다.

방화벽에서 경로항목들을 만들기

이 변환된 주소가 정확히 처리되도록 하기 위하여 몇개의 단계를 더 걸쳐야 한다. 방화벽-1이 아니라 사실상 NT가 경로기능을 제공하므로 정적NAT주소를 호스트의 합법적인 IP주소와 결합시키는 하나의 정적경로항목을 지령창에서 만듦으로써 NT를 속여 넘겨야 한다.

다음과 같은 지령을 입력한다.

Route add-p {legal IP address} mask 255.255.255.255 {Private IP address}

실례로 우편중계기에 배당된 IP주소가 192.168.1.10이고 합법적인 정적NAT주소가 206.121.73.10이라면 그 항목은 다음과 같이 나타날것이다.

Route add-p 206.121.73.10 mask 255.255.255.255 192.168.1.10

그 호스트가 그 방화벽에 국부적으로 련결되여 있는 토막에 속해 있다면 이것은 정확하다. 만일 호스트가 경로기의 밖에 있는 원천토막에 위치하고 있다면 사설IP주소항목을 경로기의 국부주소와 교체하여야 한다.

ARP와 관련한 문제들

NAT를 리용하면 OSI층 2(자료련결층)과 OSI층 3(망층)통신사이에서 변환할 때 문제가 발생할수 있다. 어떻게 문제가 발생하는가를 보기 위하여 그림 7-11에서 보여 준 망을 고찰하자. 내부망은 사설주소공간을 리용하고 있다. 이것은 우편중계기가 완전한 인터네트련결을 가지기 위하여서는 정적NAT를 리용하여야 한다는것을 의미한다.

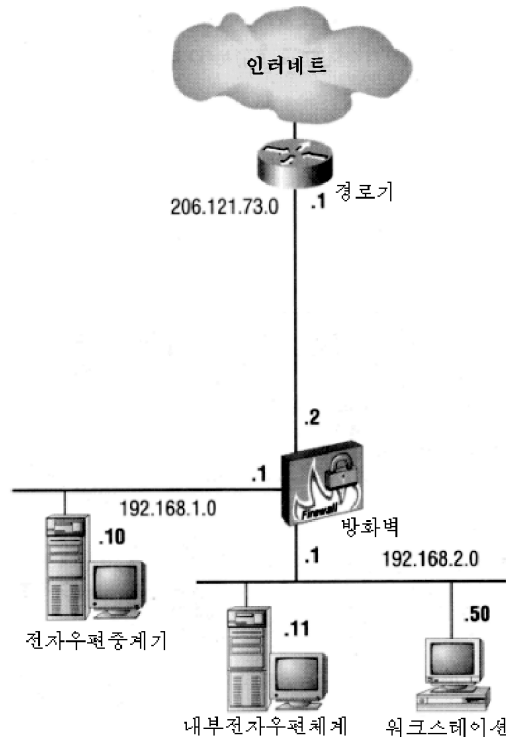



그림 7-11. 사설주소공간을 리용하는 하나의 망

이제 ISP가 하나의 류형 C주소공간 206.121.73.0을 배당하였다고 가정하자. 206.121.73.1을 경로기의 이써네트대면부에, 206.121.73.2를 방화벽의 외부대면부에 배당하고 우편중계기를 위한 정적NAT주소로서 206.121.73.10을 리용하려고 한다. 이렇게 되면 한가지 흥미 있는 일이 생긴다. 무엇이 일어 나는가를 보기 위하여 하나의 나가는 전

자우편통보문을 전송하려고 할 때의 통신대화를 따라 가 보자. 간단성을 위하여 우편중계기는 자기가 통보문을 전달하려고 하는 외부호스트의 IP주소를 이미 알고 있다고 가정하자.

우편중계기는 외부호스트에 하나의 통보문을 전송하여야 한다는것을 인식한다. 그것은 자기의 IP주소를 원천주소(192.168.1.10)로 하고 원격우편체계의 IP주소를 목적지주소(192.52.71.4)로 하여 IP머리부를 만든다. 우편중계기는 새로운 대화를 설정하기 위하여 이 초기파케트에서 SYN=1로 설정한다.

다음에 우편중계기는 192.168.1.1(자기의 기정관문설정)의 MAC주소를 위하여 ARP를 내고 이 첫 파케트를 방화벽에로 전송한다.

방화벽은 NAT표를 조사하여 이 호스트주소가 정적으로 넘기기 되여야 한다고 인정한다. 방화벽은 원천IP주소를 206.121.73.10으로 바꾸고 그 경로기의 이써네트대면부(206.121.73.1)인 자기의 기정관문설정을 위한 ARP로 낸다. 방화벽은 다음에 이 초기련결요청을 전송한다. 이 과정을 그림 7-12에서 보여 주었다.

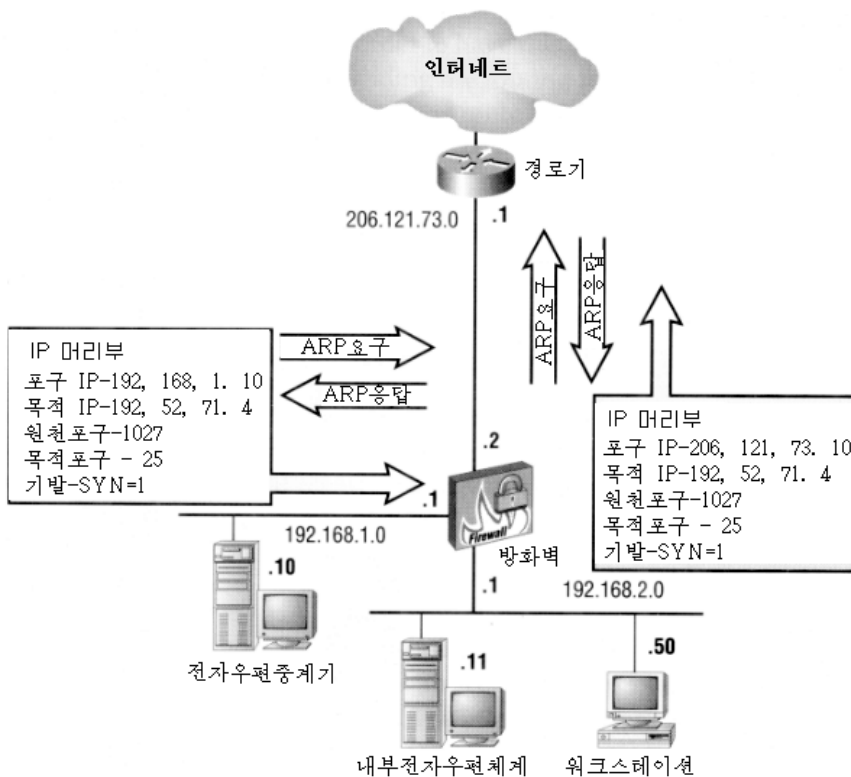



그림 7-12. 우편중계기로부터의 초기대화요청

인터네트에 의하여 이 초기자료파케트는 목적지호스트에로 경로조종된다. 원격호스트는 사실 우편체계이고 련결요청은 접수되였다고 가정하자. 원격호스트는 자기의 IP주소를 원천주소로 하고(192.52.71.4) 우편체계의 합법적인 IP주소를 목적지IP주소(206.121.73.10)로 하여 하나의 IP머리부를 만든다. 그 우편체계는 새로운 대화를 설정하려는 요청에 답례하기 위하여 SYN=1, ACK=1로 설정한다. 이 응답이 오유없이 경로

기에로 돌아 온다고 가정하자.

이 점에서 흥미 있는 문제가 제기된다. 경로기는 이 답례를 자기의 WAN포구에서 수신하고 자기의 경로표와 상담한다. 경로기는 206.121.73.0망이 자기의 이써네트포구에 직접 련결되였다고 인정한다. 이 체계가 방화벽의 다른쪽에 있다는것을 알아 차리지 못하고 그것은 206.121.73.10에 하나의 ARP를 전송함으로써 국부적전달을 시도한다. 이 주소를 리용하는 실제적인 체계는 없으므로 ARP요청은 실패한다. 경로기는 그 호스트가 정지되였다고 가정하고 원격우편체계에 오유통보를 보내준다.

어떻게 이 문제를 극복하고 경로기가 그 응답을 방화벽에 직접 전달하도록 할것인가? 다행히도 우리는 이런 상황을 개선할수 있는 몇가지 선택항목들을 가지고 있다.

경로기에서 ARP를 고치기

만일 그 경로기가 정적ARP항목들을 지원한다면 방화벽의 외부대면부의 MAC주소를 IP주소로 넘기기하는 하나의 가짜 항목을 그 경로기에 만들수 있다. 방화벽이 206.121.73.10에 대한 파케트를 수신하면 그것은 더는 ARP방송을 전송하지 않아도 된다. 경로기는 ARP캐쉬를 조사하여 만든 정적항목을 찾고 그 파케트를 방화벽에로 직접 전달한다.

만일 그 경로기가 Cisco의것이라면 다음의 명령으로 전체 구성방식에서 이 항목을 만들수 있다.

```
arp {ip address} {hardware address}
```

일러두기

방화벽의 외부MAC주소를 얻기 위하여 방화벽의 외부주소에 Ping을 보내고 경로기의 ARP캐쉬를 볼수 있다. 이렇게 하면 경로기가 기대하는 형태로 MAC주소를 연시하게 된다.

모든 경로기가 다 정적ARP항목을 만드는것을 지원하지는 않는다. 만일 이 경로기들중 어느 하나를 계속 쓰고 있다면 다른 하나를 더 선택하여 해보는것이 좋다.

경로기에서 정적ARP항목을 구성하는것의 유일한 결함은 만일 방화벽과 경로기사이에 있는 토막에 여러개의 장치들을 가지고 있다면(다른 경로기나 또는 보호되지 않는 봉사기와 같은) 이 변환된 주소에 도달하기 위해서 매 장치가 하나의 정적ARP항목을 필요로 하게 된다는것이다.

방화벽에서 ARP를 고치기

또한 NT봉사기가 변환된 주소에 따라 ARP요청에 응답하도록 함으로써 방화벽우에서 이 문제를 해결할수 있다. 이것을 대리자 ARP라고 부르며 이것은 UNIX플래트홈에서의 일반적인 특징이다. 그런데 NT는 다른 IP주소들에 대한 대리자 ARP를 수행하기 위한 내장된 방법을 가지고 있지 못하다. 다행히도 우리는 방화벽-1 쏘프트웨어를 통하여 대리자 ARP를 구성할수 있다.

주　　의

대부분의 UNIX기계들은 -p 스위치를 가지고 정적ARP를 지원한다. 이 스위치는 UNIX기계가 그 지정된 IP주소를 《발표》하게 하거나 또는 그것을 위한 대리자로서 동작하게 한다. 만일 방화벽이 UNIX우에서 돌고 있다면 이것은 NAT주소와 관련하여 ARP문제를 극복하게 될것이다.

우리의 ARP문제에서 \%fwl%\state 등록부에서 하나의 파일을 만들어야 한다. 파일의 이름은 local.arp라고 한다. 이 파일에서 매 정적으로 넘기기된 IP주소를 방화벽의 외부대면부의 MAC주소와 련관시키는 행당 하나의 항목을 만들어야 한다. 매행의 형식은 다음과 같은 모양을 가진다.

206.121.73.10　　00-00-0C-34-A5-27

체계를 재기동하면 방화벽은 목록의 항목들에 대한 ARP요청들에 응답하기 시작한다.

주　　의

이 방법의 유일한 결함은 10개 또는 그이상의 항목들을 만든다면 일치하게 동작하지 않는다는것이다. 체계가 얼마나 자주 응답할것인가 하는것은 그것이 시간상으로 얼마나 바쁜가 하는데 달려 있다. 만일 변환하여야 할 많은 IP주소들을 가지고 있다면 다른 방법들중 하나를 통하여 NT에 대한 대리자 ARP를 극복하는것을 보아야 한다.

경로변화에 의한 ARP고치기

물론 NAT주소에 대한 ARP를 수정하는 가장 쉬운 방법은 ARP가 결코 전송되지 않도록 담보하는것이다. 자기의 부분망주소체계와 경로표들을 변화시켜 경로기가 그 정적 NAT주소들이 국부적이라고 생각하지 않도록 함으로써 이것을 할수 있다.

실례로 자기의 ISP에게로 가서 이미 받은것에 추가하여 하나의 새로운 합법적인 부분망주소를 달라고 요구하였다고 하자. 완전한 류형 C주소공간을 요구하는것이 아니라 부분망마스크로서 255.255.255.252를 리용하는것을 요구한다. 대부분의 ISP들은 이 요구를 들어 줄것이다. 그것은 그 망이 두개의 호스트만을 지원하고 있고 또 ISP들은 보통 점대점WAN련결에서 리용하기 위하여 이 증가분으로 갈라 진 주소공간을 가지고 있기때문이다.

일러두기

만일 ISP가 추가적인 주소공간을 주지 않는다면 이미 받은 주소공간을 부분망으로 가를수 있다.

일단 이 주소공간을 얻었다면 그것을 리용하여 경로기와 방화벽사이에 있는 망을 처리하여야 한다. 실례로 만일 ISP가 망주소 206.121.50.64를 넘겨 주었다면 경로기의 이써네트대면부에 206.121.50.66을 리용할수 있다. 다음에 경로기에 하나의 경로항목을 만들어 206.121.73.0망에로의 가장 좋은 경로는 방화벽의 외부대면부(206.121.50.66)를 통

하는것이라고 알리게 하여야 한다.

일러두기

만일 방화벽의 외부IP주소를 변화시킨다면 새로운 사용권열쇠를 받아야 할것이다.

그러면 경로기는 더는 그것이 정적으로 넘기기한 주소들에 대하여 국부적이라고 생각하지 않게 되며 이 주소에 대한 ARP요청도 더는 보내지 않게 된다. 경로기는 자기의 경로표에 따라 이것이 국부호스트가 아니라는것을 알게 되며 따라서 그 파케트를 다음 도약에 전송하여야 하는데 다음 도약은 바로 그 방화벽이다.

방화벽-1규칙들의 동작

요구되는 망객체들을 만들었으므로 이제는 그것들을 방화벽규칙들에 리용하여 보안방책을 실현하여야 할 때가 왔다. 한가지 표본적인 방책을 그림 7-13에 보여 준다.

cam - Check Point Policy Editor

File Edit View Manage Policy Window Help

Security Policy - Standard | Address Translation - Standard

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Internal	Any	NBT	drop		Gateways	Any
2	Any	Any	tftp snmp	drop	Alert	Gateways	Any
3	Internal	Any	Any	accept	Account	Gateways	Any
4	Any	web_server	http	accept	Short	Gateways	Any
5	Any	mail_relay	smtp	accept	Short	Gateways	Any
6	mail_relay	Herne	smtp	accept	Short	Gateways	Any
7	DMZ_Network	Internal	Any	drop	Alert	Gateways	Any
8	mail_relay	Any	smtp dns	accept	Short	Gateways	Any
9	Any	DMZ_Network Internal	echo-tcp Chargen	drop	Mail	Gateways	Any
10	Any	Any	Any	drop	Long	Gateways	Any

Save completed successfully! cam Read/Write NUM

그림 7-13. 표본적인 방화벽-1규칙들

이 규칙들은 왼쪽으로부터 오른쪽으로 가면서 읽는다. 실례로 규칙 4는 다음과 같은 내용을 서술하고 있다. 《포구 80으로 체계 web-server에 련결하는 임의의 IP호스트는 방화벽에서 허용되여야 한다.》 포구 80은 HTTP를 위한 잘 알려 진 포구이다. 방화벽-1은 그저 파케트머리부들을 조사하는것이 기본이라는것을 알아야 한다. 원격체계가 실지로 HTTP요청을 전송하고 있는가를 알기 위한 방법이 없다. 봉사렬은 리용을 쉽게 하기 위

하여 포구번호대신에 봉사이름을 사용하고 있다. 아래에 매개 렬에 대한 서술을 준다.

No 기준을 제공하기 위하여 매개 규칙을 번호로 표시한다.

Source 이 규칙에 의하여 영향을 받게 되는 원천호스트 또는 망을 표시한다.

Destination 이 규칙에 의하여 영향을 받게 되는 목적지호스트 또는 망을 표시한다.

Service 이 규칙의 영향을 받는 봉사포구번호를 표시한다.

Action 원천, 목적지 그리고 봉사를 한조합으로 하였을 때 파케트에 대하여 무엇이 진행되는가를 결정한다. 선택항목들은 다음과 같다.

Accept 통과시킨다.

Drop 원천에 알리지 않고 그 파케트를 제거

Reject RST=1인 파케트를 그 원천에 보낸다.

User Auth 련결을 위하여 사용자인증을 실시

Client Auth 련결을 위하여 의뢰기인증을 실시

Session Auth 련결을 위하여 대화인증을 실시

Encrypt 나가는 파케트를 암호화하고 들어 오는 파케트를 받아 들이고 부호화한다.

Client Encrypt SecuRemote(Check Point의 VPN의뢰기)통신만을 허용

Track 이 규칙이 정합될 때 무엇이 진행되여야 하는가를 결정한다. 선택항목들은 다음과 같다.

Ignore 그림기호에 의하여 표시되지 않는다. 이 항목을 비워 놓으면 등록파일항목을 만들지 않는다.

Short log entry 원천IP주소와 목적지IP 그리고 포구주소를 기록한다.

Long log entry 우의 항목에 원천포구와 파케트크기를 더 기록한다.

Account 계산등록파일에 항목을 쓴다.

Alert 특수한 미리 정의된 작용을 한다.

Mail 등록파일항목을 포함하는 하나의 전자우편을 보낸다.

SNMP Trap 하나의 SNMP통보를 넘긴다(Properties Setup창문의 Log and Alert에서, SNMP Trap Alert 마당에서 정의된).

User defined 사용자의 주문에 따르는 동작을 수행한다.

Install On 어느 체계에 대하여 그 규칙항목이 집행되여야 하는가를 정의한다. 기정은 관문인데 이것은 관문으로서 정의된 모든 망객체들을 포함한다. 또한 매 규칙을 선택적으로 설치할수 있다.

DST 목적지로 정의된(보통 봉사기) 망객체들에서 들어 오는 자료흐름을 표현

Src Dst와 류사한데 나가는 자료흐름을 표현한다(그것은 의뢰기에서 시작된다.).

Router 규칙들은 모든 경로기들에서 집행된다.

Integrated FireWall 규칙들은 모든 통합된 방화벽들에서 집행된다.

Target 규칙들은 들어 오는 그리고 나가는 자료흐름들에서 특정의 목표에 적용된다.

Time 이 규칙이 어느 시간, 요일, 날자에 집행되여야 하는가를 결정한다. 실례로 규칙 3에서 Time이 5:00 PM to 8:00 AM으로 변경되였다면 사용자는 작업시간 이후에만 인터네트에 접근할수 있다. 여러개의 시간객체를 가질수 있는 새로운 집단객체를 만들수도 있는데 이것은 특정의 규칙에 집체적으로(집단으로서) 적용된다.

Comments 규칙의 목적을 서술하는 본문을 첨부할수 있게 한다(이 렬은 그림 7-13에서 부분적으로만 보여 준다.).

규칙모임에 대한 리해

그림 7-13에서 보여 준 매 규칙들을 간단히 고찰하자. 이 규칙들이 자기의 환경에 적합하다고 생각되면 자유롭게 적용할수 있다.

규칙 1은 내부망으로부터 시작하는 모든 NetBIOS자료흐름들을 막되 등록파일에 등록하지 말것을 방화벽에 지시한다. Windows기계들은 분당 한번씩 이름정보를 방송한다. 이 항목들은 등록파일을 빨리 채울수 있으며 실제로 관심하는 정보들을 제거하기 어렵게 만든다. Track렬을 공백으로 하면 등록파일에 이 자료흐름을 기록하지 않는다.

규칙 2는 방화벽을 절대 통과하지 못하게 하려는 봉사를 막는데 리용된다. 이것은 침입의 효과를 최소화하는데 리용될수 있다. 실례로 Web봉사기가 공격을 받아 손상되였다고 하자. 공격자는 내부환경에 대한 보충적인 정보를 얻기 위하여 원격위치에로 SNMP정보를 전송하려고 시도할수 있다. 대부분의 기관들은 인터네트접근과 관련하여 보통 매우 완만한 방책을 가지고 있으므로 이 정보는 망을 떠나도록 허용될것이다. 규칙 2는 이 자료흐름을 막을뿐아니라 관리자에게 어떤 수상한 일이 생겼다는것을 알린다.

규칙 3은 앞의 규칙들에 의하여 차단된 봉사들을 제외하고 내부체계가 요구되는 임의의 형식의 통신을 수행할수 있게 한다. 경로기접근목록과 마찬가지로 방화벽-1은 규칙들을 순서대로 처리하며 자료흐름들은 가장 잘 맞는 조건에서가 아니라 처음으로 맞는 조건에 기초하여 평가된다.

규칙 4와 5는 각각 Web봉사기와 우편중계기로 가는 허용가능한 자료흐름을 받아 들이게 한다. 이 체계들은 격리된 DMZ에 위치하고 있기때문에 규칙 6은 우편중계기가 내부우편체계에로 SMTP통보문들을 전달하게 한다.

이 규칙과 규칙 7이 결합되면 DMZ로부터 내부망에로 가는 다른 자료흐름들은 허용되지 않는다. 또한 이것은 공개봉사기들중 하나가 손상되였을 때 내부망을 보호하는데서도 도움이 된다.

규칙 8은 우편중계기가 인터네트밖에 있는 호스트들에 통보문을 전달하도록 하는데 리용된다.

규칙 9는 수상한 활동들을 찾는다. 특히 TCP echo와 문자발생기봉사에 련결하려고 시도하는 자료흐름들을 찾는다. 이 봉사들은 많은 경우 약점으로 되는것으로 알려 져 있다. 내부체계들은 사실상 이 봉사를 제공하지 않는다. 규칙 9는 특히 스캐너와 같은 어

떤것이 망을 조사하고 있지 않는가를 감시하도록 설정되였다. 이러한 자료흐름이 검출된다면 방화벽이 간단히 하나의 등록파일항목을 만드는것으로 그치는것이 아니라 추가적인 작용을 취하도록 하여야 한다.

그러면 왜 모든 리용되지 않는 포구들을 감시하지 않는가? 만일 공격자가 포구스캐너를 사용하고 있다면 이 규칙은 수백수천번 평가될수 있다. 바라는것은 방화벽이 진행중의 공격을 경고할 때 우편체계가 봉사거절을 하도록 하는것이다.

규칙 10은 무조건적인 거부이다. 이 규칙은 다음과 같은 내용을 규정하고 있다. 《우에서 언급된 규칙들중 하나라도 맞지 않는 모든 자료흐름은 거부된다.》

규칙들의 변경

한개 행을 추가하여 새로운 규칙항목을 만들기 위하여 Edit menu선택항목을 선택한다. 매 새로운 행은 다음과 같은 기정의 규칙을 가지고 만들어 진다. 《모든 자료흐름은 거부한다.》 파라메터들을 변화시키기 위하여 매개 칸에서 오른쪽찰칵을 하고 Add를 선택한다.

실례로 한 규칙에서 Source항목을 변경시키기 위하여 Source칸에서 오른쪽찰칵을 하고 내리펼침차림표에서 Add를 선택한다. 그러면 이 새 규칙의 원천파라메터들을 규정하는데 첨가할수 있는 적절한 객체들의 목록이 나타난다. 보안방책을 실현하는데 필요한 모든 규칙들을 만들 때까지 이 과정을 계속하면 된다.

방화벽속성변경

규칙기지는 자료흐름파라메터들을 구성하는데 필요한 유일한 장소가 아니다. 방화벽그자체의 속성들을 변경시킬수도 있다. 이것을 하기 위하여 Security Policy−1차림표로부터 Policy→Properties를 선택한다.

Properties Setup화면을 그림 7−14에서 보여 준다.

주 의

> 이 화면은 규칙기지 밖에서 처리되여야 하는 자료흐름들을 정의하므로 좀 복잡하다. 다른 말로 하면 규칙기지편집기안에서 특별히 정의되지 않았다고 해도 처리되여야 하는 봉사들을 정의한다.

Accept RIP항목이 기정으로 선택되지 않는다는것을 주목하여야 한다. 이 선택항목은 방화벽에 다음의 내용을 요구하는것이다. 《규칙기지를 처리하기전에 RIP자료흐름을 접수하라.》 방화벽에 RIP갱신들을 접수하도록 요구하는 규칙을 가지고 있지 않아도 어쨌든 방화벽은 그렇게 할것이다. 만일 공격자가 망에서 방화벽−1을 사용하고 있다는것을 안다면 그것은 경로표를 혼란시키기 위하여 그 방화벽에 틀린 RIP갱신들을 전송하려고 시도할수 있다. 이것은 가능할 때마다 정적경로조종이 리용되여야 한다는 또 하나의 리유로 된다.

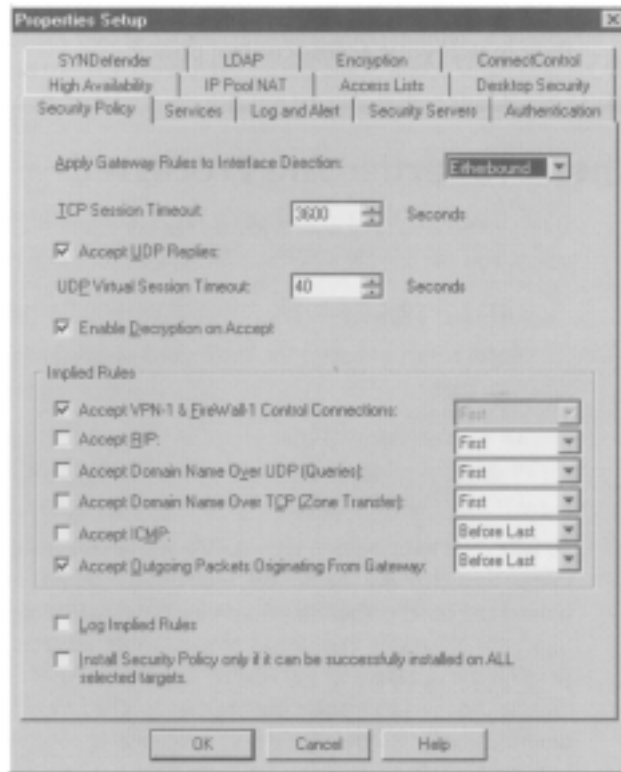



그림 7-14. Properties Setup화면

다른 Properties Setup표쪽들에서 가능 또는 불가능으로 할수 있는 봉사들이 있다. Services and Access Lists표쪽을 검열하여 그것들이 망의 접근조종방책과 일치하도록 담보되였는가를 확인하여야 한다.

속성들은 언제 처리되는가?

망의 보안방책과 일치하도록 이 속성들을 구성하지 않는다면 이것은 중요한 보안상의 구멍으로 된다. 다음의 설정들을 리용하여 매 속성들이 언제 처리되는가를 규정할수 있다.

First 규칙기지를 처리하기전에 이 자료흐름을 접수

Before Last 규칙기지가 특별히 그것들을 막지 않는 한 이 자료흐름을 접수

Last 규칙기지에서의 마지막규칙후에 이 자료흐름을 처리. 만일 그것이 특별히 차단되지 않는다면 통과시킨다. 만일 마지막규칙이 《임의의 원천으로부터 임의의 목적지로 가는 모든 자료흐름을 막으시오.》 하는것이면 이 속성은 평가되지 않는다.

그러면 왜 이것이 보안에서 중요한 착오로 되는가?

생활에서 보는 많은 문제들에서와 같이 보안도 방화벽을 보다 사용하기 쉽게 하려는 노력에 의하여 약화될수 있다(물론 가장 낮은 공통분모를 요구하지만).

실례로 방화벽관리자는 자기가 경로갱신을 처리하기 위하여 RIP자료흐름을 허용하여야 한다는것을 리해하지 못할수 있다. 관리자는 리해력이 좀 느려서 내부체계가 호스트이름을 IP주소로 변환할수 있도록 하기 위하여서는 DNS질문들을 통과시켜야 한다는것을 깨닫지 못할수 있다. 이러한 속성들은 우와 같은 오유들을 피하기 위하여 기정에 의하여 가능으로 만들수 있다. 소비자의 교육을 개선할대신에 회사들은 자기들의 제품이 제공하는 보안의 수준을 맞춤으로써 이것을 보상한다.

SYNDefender표쪽

평가하여야 할 마지막Properties Setup표쪽은 SYNDefender표쪽이다. SYNDefender는 방화벽이 내부체계를 SYN에 기초한 공격으로부터 보호한다.

제3장에서 TCP통신을 고찰할 때 두 호스트가 대화를 시작하기전에 TCP련결신호를 교환한다는것을 보았다. 이 련결신호를 주고받는 동안에

1. 원천지는 목적지에 SYN=1인 하나의 파케트를 보낸다.
2. 목적지는 원천지에 SYN=1, ACK=1로 응답한다.
3. 원천지는 목적지에 ACK=1인 하나의 파케트를 보낸다.
4. 원천지는 자료전송을 시작한다.

주 의

TCP호스트는 두개의 통신대기렬을 가지고 있는데 작은것은 TCP련결신호를 실현하는 대화를 위한것이고 큰것은 완전히 설정된 대화를 위한것이다. SYN공격의 목표로 되는것도 작은 대기렬이다.

목적지호스트가 첫 SYN=1파케트를 수신하면 그것은 이 련결요청을 작은 《처리중》 대기렬에 보관한다. 대화설정은 좀 빨리 진행되게 되여 있으므로 이 대기렬은 작고 비교적 적은수의 련결요청들만을 보관할수 있다.

SYN공격은 이 작은 대기렬을 련결요청들로 차넘치게 한다. 목적지체계가 하나의 응답을 넘길 때 공격하는 체계는 응답하지 않는다. 이것은 그 련결요청이 시간한계가 초과되고 그 항목이 제거될 때까지 그 작은 대기렬에 남아 있게 한다. 이 대기렬을 가짜련결요청들로 가득 채움으로써 공격하는 체계는 그 체계가 합법적인 련결요청들을 받지 못하게 한다. 그러므로 SYN공격은 봉사거부공격으로 간주된다.

SYNDefender표쪽은 이 문제를 해결하기 위한 두가지 방도를 제공한다. 방화벽이 다음의 두가지로 기능하도록 구성할수 있다.

- 피동 SYN관문
- SYN관문

피동SYN관문으로서 방화벽은 들어 오는 련결요청들을 대기하다가 응답 SYN=1, ACK=1파케트를 전송체계호스트에로 속여서 돌려 보낸다. 이것은 련결요청이 내부체계에 도달하지 못하게 한다. 적당한 ACK=1이 전송체계로부터 수신되면 방화벽은 내부체계와 련결신호를 나누고 두 호스트사이에서 자료흐름을 통과시키기 시작한다. 결과적으로 방화벽은 SYN대리자와 같이 동작하는것으로 된다.

이 방법의 결함은 초기대화설정에서 약간의 지연이 있는것이다. 또한 방화벽이 모든 련결요청들을 다 중재하므로 방화벽에서 많은 처리가 요구된다. 실례로 하나의 Web열람기는 Web페지를 내리적재할 때 여러개의 대화를 만들수 있다. 도형, 본문 그리고 그림기호에 대하여 각각 하나의 대화가 설정될수 있다. 가장 인기 있는 싸이트들은 최소 50개의 대화를 만들고 있으며 그림이 많은 어떤 싸이트들은 300개의 동시적인 련결을 만드는것도 있다. 추가적인 보호로서 피동SYN관문은 시간한계(기정값은 10s)와 허용되는 최대대화수(기정값은 5000)를 규정할수 있게 한다.

다른 하나의 방법은 방화벽을 SYN관문으로 설치하는것이다. 이 방식에서 방화벽은 SYN=1요청과 SYN=1, ACK=1응답이 그 방화벽을 그저 통과하게 한다. 그러나 이 점에서 방화벽은 련결요청을 완성하고 그 대화를 큰 대기렬로 이동시키기 위하여 내부체계에 ACK=1로 응답할 때 방화벽은 이 한 파케트는 막고 그 대화의 나머지는 정상적으로 허용한다.

원격호스트가 상당한 시간동안 응답하지 않는다면 방화벽은 내부체계에 RST=1을 보내여 그 대화를 끝낸다. 여기서 유일한 문제는 공격이 진행되고 있다면 요구되지 않는 대화를 내부체계에 만들어 놓을수 있다는것이다. 이것은 전형적인 문제로는 되지 않는다. 그것은 동작중의 대화대기렬은 여러 대화들을 보다 쉽게 취급할수 있기때문이다.

이 방법은 또한 SYN중계기방법에서 생기는 설정지연문제를 해결할수 있다.

보안봉사기의 동작

보안봉사기는 방화벽이 특정봉사를 위한 련결을 대리하게 하며 자료흐름조종을 더 잘할수 있게 한다. 이것은 리용되고 있는 봉사가 아니라 자료의 내용에 기초하여 려과결정을 하려고 할 때 쓸모가 있다.

실례로 InterNIC에 등록된 다음과 같은 3개의 령역이름들이 있다고 가정하자.: foobar.com, fubar.com, bofh.com

foobar.com이 기초령역이름이지만 이 3개의 령역모두에 대하여 우편을 수신하려고 한다. 이것은 매 사용자에게 적용하면 ftuttle @ foobar.com, ftuttle @ fubar.com 그리고 ftuttle @ bofh.com은 다 같은 사람에게로 경로조종되여야 한다. 그러나 나가는 우편은 항상 foobar.com령역에서 시작되는것으로 나타나야 한다.

우편봉사기가 여러개의 령역들을 취급하도록 구성하려고 한다면 많은 일을 하여야 한다. 많은 우편봉사기들은 매 사용자에 대하여 3개의 서로 다른 우편주소들을 구성할것을 요구한다. 보통 첫번째것은 자동적으로 만들어 지며(ftuttle @ foobar.com과 같이) 다른 두개에 대해서는(ftuttle @ fubar.com과 ftuttle @ bofh.com) 별명을 수동으로 만들어야 한다. 이 추가적인 항목들은 관리시간을 증가시키고 타자오유나 항목을 빠뜨리는것과 같

은 오유가능성을 끌어 들이게 된다.

오랜 우편봉사기들은 여러개의 우편령역들을 관리하는 능력을 가지고 있지 못하다. 우편관리자는 오랜 우편봉사기들에 하나의 우편령역만을 구성할수 있다. 이것은 다른 령역에로 우편이 향하게 하거나 거절되게 할수 있다.

한가지 보다 간단한 해결책은 SMTP보안봉사기를 구성하여 목적지령역이름에 대하여 들어 오는 우편들을 분석할수 있게 하는것이다. 만일 령역이름 fubar.com 또는 bofh.com이 검출되였다면 보안봉사기가 령역이름 foobar.com으로 그것을 교체하게 할수 있다. Foobar.com에로 주소지정된 우편은 변경없이 통과할수 있다. 이것은 우편봉사기에 도착하는 모든 들어 오는 우편통보문들이 항상 foobar.com이라는 목적지령역주소를 가질것이라는것을 의미한다. 우편봉사기는 하나의 령역이름만을 알고 있으므로 매 사용자에 대하여 또 다른 우편주소를 만들지 않아도 된다.

SMTP보안봉사기를 구성하기

SMTP보안봉사기를 리용하기 위하여서는 먼저 방화벽-1 구성도구프로그람을 통하여 그것을 가능하게 하여야 한다. 방화벽-1 구성도구에 대한 절에서 이 봉사기를 어떻게 가능으로 하는가를 고찰하였으며 이것을 그림 7-5에서 보여 주었다. 일단 SMTP보안봉사기가 가능으로 되면 Security Policy-1표쪽에서 SMTP자원들을 정의하여야 한다. Security Policy-1표쪽의 기본차림표에서 Manage→Resources를 선택한다. 그러면 Resource Management화면이 나타난다. 이것을 처음으로 돌린다면 그것은 아무런 항목도 포함하고 있지 않을것이다. New를 찰칵하고 SMTP를 선택한다. 그러면 그림 7-15에 보여 준 SMTP정의칸이 나타날것이다.

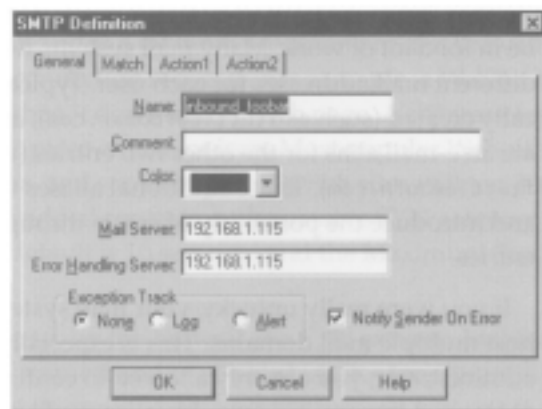



그림 7-15. SMTP의 General표쪽

foobar.com에 전송된 들어 오는 우편을 취급하는 자원을 구성하는것부터 시작한다. Inbound_foobar와 같은 서술적이름을 리용할수 있는데 이 정의는 그것이 일단 보안방책에 첨가된 이상 쉽게 인식될수 있다. 우편봉사기마당에서 우편을 전송하려고 하는 우편봉사기의 IP주소를 입력한다(지금우편배달에 IP주소를 리용하라. 방화벽은 호스트이름을 변환하지 않아도 된다.). Error Handling Server마당에서 오유통보문을 전송하려고 하는 우

편체계의 IP주소를 입력한다. 이것은 Mail Server마당에서 정의한 IP주소와 같은것일수 있다.

Exception Tracking은 이 자원이 처리하는 모든 전자우편통보문들을 등록파일에 등록할것인가를 정의한다. 하나의 경보를 보내는 선택항목도 있다. 또한 Notify Sender On Error검사칸을 선택할수 있는 선택항목을 가지고 있다. 만일 그 자원이 들어 오는 우편통보문과 맞는데 보안봉사기는 그 통보문을 전달할수 없다면 이것을 검사하는것은 하나의 오유통보문이 원래의 송신자에게 보내졌다는것을 의미한다.

이제는 그림 7-16에서 보여 준것처럼 Match표쪽을 구성할수 있다.

Match표쪽의 구성은 매우 간단하다. Sender 또는 Recipient마당에서 이 자원과 맞추려고 하는 본문을 입력한다. 별표(*)는 만능기능으로 동작하며 임의의 문자렬과 정합될수 있다. Recipient마당은 @ foobar.com으로 끝나야 한다. 이것은 foobar.com령역을 위하여 모든 들어 오는 우편들을 맞추어 볼것이다.

전자우편의 머리부에 그 어떤것을 다시 쓰지 않도록 하기 위하여 이 특수한 자원을 구성하게 된다. 간단히 OK를 찰칵하면 이 항목이 기억된다.

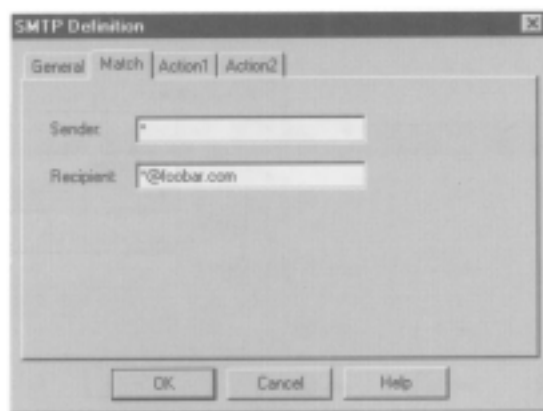



그림 7-16. SMTP의 Match표쪽

이제는 별명을 만들기를 원하는 령역들에 대한 항목들을 만들어야 한다. Resource Management화면으로부터 New를 다시 찰칵하고 SMTP를 선택한다. 그러면 그림 7-17에 보여 준것과 같은 새로운 SMTP Definition칸이 나타나게 된다.

General표쪽을 선택하고 이 자원에 서술적인 이름(inbound-fubar.com과 같은)을 준다. Fubar.com으로 주소지정된 우편은 foobar.com과 같은 우편체계에 전달되므로 foobar.com 항목에서 리용된것과 같은 Mail Server 및 Error Handling Server IP주소를 입력한다.

Match표쪽에서 Sender마당을 패턴정합하기 위하여 다시 별표(*)를 사용하지만 Recipient마당은 항목 * @ fubar.com을 포함할것이다. 이렇게 하면 이 또하나의 령역이름에로 전송된 들어 오는 전자우편주소들을 패턴정합할수 있게 된다. 이것은 다시 쓰려고 하던 령역이름들중의 하나이므로 그림 7-17에 보여 준 Action 1표쪽을 변경시켜야 한다.

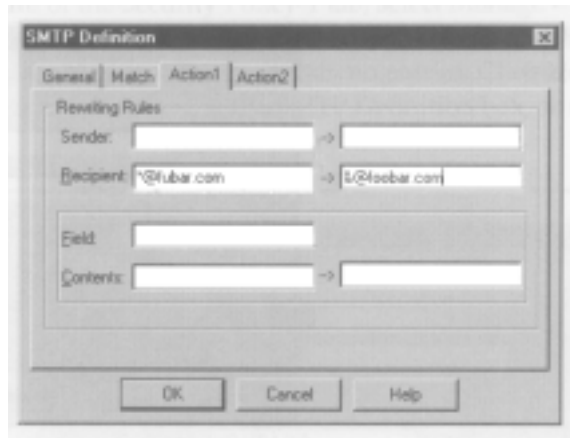



그림 7-17. SMTP정의칸의 Action1표쪽

Action1표쪽에서 써넣어야 할 마당은 Rewriting마당들뿐이다. 공백으로 되여 있는 마당들은 그대로 둬둔다. 왼쪽의 마당들은 전자우편머리부의 지정된 부분안에 있는 본문을 정합하려고 시도한다. 오른쪽의 마당들은 만일 패턴정합이 발생한다면 이 본문이 무엇으로 변경되여야 하는가 하는것을 포함한다.

첫번째 Recipient마당은 문자렬 * @ fubar.com을 가지고 있다. 이것은 재쓰기하려고 하는 주소의 부분이다. 오른쪽의 Recipient마당은 문자렬& @ foobar.com을 가지고 있다.

《&》표시는 자원에 《이전의 마당에서 별표(*)의 값을 복사하여 그것을 여기에 붙이시오.》라는것을 요구하고 있다. 이렇게 하면 새로운 수신자머리부에서 같은 사용자이름을 유지할수 있다. 나머지 본문은 그저 자원에 fubar.com을 foobar.com으로 바꿀것을 요구한다.

이것은 들어 오는 fubar.com우편에 대한 SMTP자원의 구성을 완성한다. 다음에 OK를 눌러 Resource Management화면에로 돌아 간다. Bofh.com에 대한 SMTP자원도 만들어야 한다. 여기서는 fubar.com자원을 만들 때와 같은 과정을 반복하되 이름과 패턴정합정보를 bofh.com으로 바꾸어야 한다. 완성되면 Resource Management화면을 닫고 이 자원들을 보안방책과 결합시키기 위하여 Security Policy-1 표쪽에로 간다.

그림 7-18은 매우 간단한 보안방책에 추가된 SMTP자원들을 보여 준다. 행 1은 방화벽을 통과시키려고 하지 않는 모든 자료흐름을 막는다. 행 2는 매우 완만한 보안방책을 정의하는데 이것은 모든 내부체계들이 인터네트에 있는 임의의 봉사에 접근할수 있게 한다(행 1에서 지적된것은 제외).

행 3은 SMTP자원들을 포함하는 항목이다. 이 규칙은 임의의 체계는 skylar(방화벽)에 련결할수 있고 SMTP통보문을 배달할 시도를 할수 있다는것을 지적한다. 그러면 모든 SMTP통보문은 앞에서 만든 3개의 SMTP자원들에 의하여 처리된다. 매개 자원은 행 3의 Service칸에서 오른쪽찰칵하고 ADD With Resource→SMTP를 선택하고 다음에 자원목록에서 보여 준 자원의 이름을 선택함으로써 이 규칙에 첨가된다.

우편봉사기는 행 2에 따라 완전한 인터네트접근을 가지므로 나가는 SMTP자원은 구성하지 않아도 된다. 그 우편체계는 모든 나가는 우편을 직접 완전히 전송할수 있어야 한다.

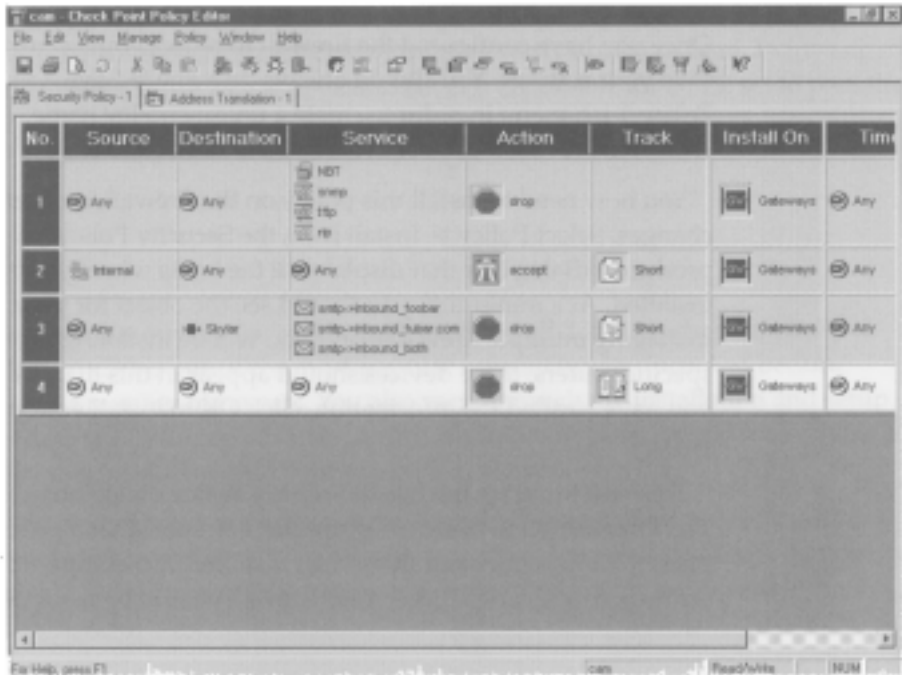



그림 7-18. SMTP자원을 리용하는 보안방책

일러두기

현재의 규칙기지의 한가지 부가적인 리득은 그것이 우편체계가 스팸중계기로 리용되지 않게 한다는것이다. 방화벽은 3개의 령역들중 하나에로 가는 통보문만을 허용할것이다. 내부우편체계에는 인터네트로부터 직접 도달할수 없다. 이것은 우편체계들중 어느것도 여러 수신자에게 광고를 중계하는 스팸중계기로 리용될수 없다는것을 의미한다.

규칙들의 설치

일반 보안방책을 반영하여 방화벽을 구성하였다면 그 설정들을 기억시켜야 한다. 일의적인 방책이름을 만들기 위하여 Security Policy-1의 차림표에서 항상 File→Save As를 선택하여야 한다. 이렇게 하면 후에 이전의 방책을 재기억시키는 경우에 일부 수정조종을 할수 있게 해준다.

앞에서 만든 변화들을 기동시키기 위하여 방화벽에 이 방책을 설치하여야 한다. Security Policy-1차림표에서 Policy→Install을 선택한다. 그러면 방화벽방책이 설치될 모든 호스트들을 연시하는 하나의 대화칸이 나타나게 된다. 최소로 자기의 방화벽에 대한 객체를 보아야 한다. 만일 여러개의 방화벽을 관리하고 있거나 또는 특정의 경로기에 접근조종목록을 설치하고 있다면 이 장치들도 이 대화칸에 나타나야 한다. 이 정보를 확인하면 방책들을 선택된 호스트들에 설치하기 위하여 OK를 찰칵한다.

그러면 그림 7-19에 보여 준 Install Security Policy대화칸이 나타날것이다. 이 대화칸의 정보는 방책서술이 오유없이 콤파일되였으며 그것이 방화벽에 성과적으로 설치되였다는것을 알리는것이다. 오유가 나타나지 않았다면 Close를 찰칵한다. 그러면 이 방화벽은 사용할 준비가 된것으로 된다.

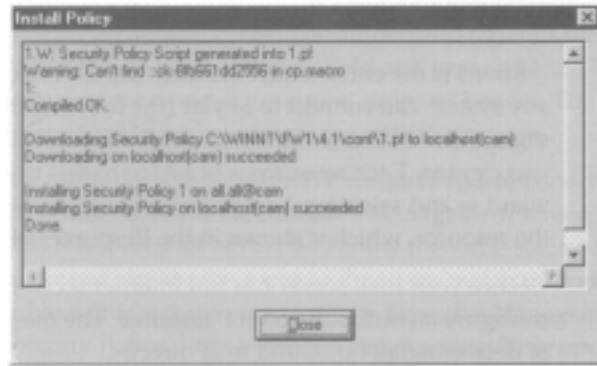



그림 7-19. Install Security Policy대화칸

오유가 나타나면 오유통보문을 구체적으로 보아야 한다. 보통 오유는 규칙들의 충돌로 인하여 생긴다. 실례로 하나의 규칙이 한 특정의 체계에 대하여 완전한 인터네트접근을 가진다고 정의하고 있는데 후에 그 같은 체계가 FTP리용이 허용되지 않는다고 정의하면 충돌이 발생하게 된다.

규칙기지를 설치할 때 방화벽은 먼저 충돌이 없는가를 검사한다. 만일 당신이 규칙들을 설치하기전에 규칙충돌이 없는가를 확인하려고 한다면 Policy→Verify 항목을 선택할수 있다. 그러나 경험에 의하면 이 검사는 충분하지 못하다. 규칙모임이 Verify검사를 통과하는것이 가능하며 다만 설치과정의 문제만을 보여 준다.

요 약

이것으로 Check Point 방화벽-1에 대한 고찰을 끝마친다. 이 장에서 우리는 방화벽-1이 왜 가장 인기 있는 방화벽제품들중의 하나로 되고 있는가를 보았다.

또한 Windows NT봉사기에서의 설치 및 설정과정들도 고찰하였다. 이제는 이 제품을 자기의 망환경에 어떻게 배비할것인가에 대하여 잘 알게 되였다.

다음장에는 망경계선안에서 보안을 조종하는 방법들을 고찰한다. 침입검출체계가 방화벽과 결합되여 매우 안전한 환경을 창조할수 있다는것을 보게 될것이다.

제8장. 침입검출체계

침입검출체계(IDS)는 최근에 출판물들에 많이 실리고 있는 아주 새로운 기술이다. 이 기술은 3～4년밖에 안되였지만 망보안에서 혁신적변혁을 가져 올수 있다는 약속을 개발자들과 할수 있을 정도로 전망이 크다. 사실상 어느 한 개발자는 자기들이 만든 IDS가 방화벽에 대한 요구를 완전히 취소한다고 대담하게 선언하였다.

분명히 IDS는 현존의 보안구조를 교체함이 없이 그 기능을 높이는 방법이라고 볼수 있다.

IDS에 대하여 자주 제기되는 질문

침입검출체계를 리해하기 위하여 여러명의 망규약전문가가 망분석기를 가지고 망자료흐름을 감시하고 있다고 생각하자. 이 전문가들은 공격자가 공격을 시도하는 전 과정을 살피면서 어떤 이상한 자료흐름이 망에 발생하면 그것을 알아 내기 위하여 매 자료묶음을 부지런히 검사한다. 만일 이상한 자료흐름을 발견하면 그들은 인차 망관리자에게 발견한 내용을 통보한다.

이러한 방식으로 사람의 기술을 대신하는 침입검출체계가 확립되게 된다. IDS는 망분석기와 같이 망으로 통과하는 모든 자료흐름을 장악한다. 일단 이 정보를 기억기로부터 읽었다면 체계는 이미 알려 진 많은 공격모형들과 그 파케트를 비교한다. 실례로 어느 한 호스트가 접속완결시도가 없이 다른 호스트에로 SYN묶음들을 반복해서 보내고 있다는것을 알게 되면 IDS는 이것을 SYN공격으로 판단하고 적절한 대응책을 취하게 된다. 좋은 IDS는 자기의 자료기지에 침입한 100개이상의 공격에 대처할수 있다.

대응작용은 현재 리용하고 있는 구체적인 IDS체계와 그것을 어떻게 구성했는가에 관계된다. 모든 IDS체계들은 비정상사건들을 관리에 기록하는 기술을 가지고 있다. 일부 체계들은 망관리자가 후에 해석할수 있도록 새로운 자료흐름묶음을 획득하여 기억시킨다. 다른것들은 전자우편통보 또는 본문과 같은 경보를 보내도록 구성되여 있다.

많은 IDS체계들은 련결의 량끝을 재시동함으로써 이상한 전송을 중단하게 할수도 있다.

또한 려과규칙을 변경시키고 공격콤퓨터를 봉쇄하기 위하여 방화벽 또는 경로기와 호상작용하는것들도 일부 있다.

이 매개 작용들에 대한 우결함들을 이 장의 마지막에 상세하게 서술하였다.

IDS는 보통 2개의 부분으로 가른다.

- **수감기** 이것은 자료흐름을 보관하고 분석하는 기능을 수행한다.
- **조종탁** 이 조종탁을 통하여 수감기를 관리하며 모든 보고기능이 실행된다.

침입검출체계들은 매우 많은 자원을 소비한다.

개발자들은 보통 256MB의 RAM과 인텔 300MHz 펜티움Ⅲ 혹은 Pro processor(또는

수감기가 UNIX에서 가동하는 경우에는 RISC방식처리기)를 장비한 체계우에서 수감기를 동작시킬것을 권고하고 있다. IDS가 모든 자료흐름을 기입하기때문에 많은 디스크공간이 자체자료기지용으로 요구된다. 대략 100MB의 디스크공간이 보통 권고되지만 자료기지를 자주 지워 버리지 않거나 또는 망을 통한 자료흐름이 많은 경우 총적으로는 더 많이 리용할것을 계획하여야 한다.

조종탁을 가동시키는 체계에 대한 요구는 매개 수감기자료기지를 복사하는데 필요한 디스크공간을 충분히 남겨 두어야 한다는것외에는 대체로 갈다.

IDS의 제한성

지금까지는 IDS가 아주 좋은 보안장치인것처럼 말해 왔지만 이러한 체계들도 완전하지는 못하며 자체의 제한성들을 가지고 있다. 사실상 잡지 Infoworld의 대중특별기고란의 한 저자는 IDS가 2000년말에 가서 생명력을 잃는다고 선언하였다.

교환망기술, 불완전한 공격징후맞추기, IDS체계들에 과부하를 주는 대량의 망자료흐름 그리고 IDS체계에서 나오는 공격통보를 숨길수 있게 암호화된 망자료들이 그렇게 말할수 있는 리유로 된다. IDS체계들이 제때에 간단히 응답하면서 공격을 막을수는 없다. 그 리유를 알기 위하여 보통의 봉사거부공격(DoS)이 어떻게 발생하는가를 보자.

눈물방울공격

눈물방울(Teardrop)공격이 체계에 대항하여 어떻게 리용되는가를 리해하기 위하여서는 먼저 IP머리부안에 토막화편기마당과 길이마당을 두는 목적을 리해하여야 한다. IP머리부를 그림 8-1에 제시하였다.

토막화편기마당은 보통 경로기에서 리용된다. 만일 경로기가 다음 토막에 관하여 너무 큰 파케트를 받는다면 경로기는 그것을 통과시키기전에 자료를 토막쳐야 한다.

```
Packet Number : 13          3:52:02 PM
Length : 66 bytes
ether: ==================== Ethernet Datalink Layer ====================
       Station: Skylar ----> This_Workstation
       Type: 0x0800 (IP)
   ip: ====================== Internet Protocol ======================
       Station:10.1.1.100 ---->10.1.1.25
       Protocol: TCP
       Version: 4
       Header Length (32 bit words): 5
       Precedence: Routine
             Normal Delay, Normal Throughput, Normal Reliability
       Total length: 48
       Identification: 21249
       Fragmentation not allowed, Last fragment
       Fragment Offset: 0
       Time to Live: 128 seconds
       Checksum: 0x9148(Valid)
  tcp: ================ Transmission Control Protocol ================
       Source Port: 258
       Destination Port: 1027
       Sequence Number: 417610
       Acknowledgement Number: 898472
       Data Offset (32-bit words): 5
       Window: 8510
       Control Bits: Acknowledgement Field is Valid (ACK)
             Push Function Requested (PSH)
       Checksum: 0x5DB5(Valid)
       Urgent Pointer: 0
```

그림 8-1. IP머리부해신

토막화편기마당은 길이마당과 함께 리용된다. 그래야 수신체계가 정확한 순차에 따라 자료통보문을 재결합할수 있기때문이다.

토막화편기값으로 0이 수신되였다면 수신체계는 이것이 첫번째 토막친 정보묶음이든지 아니면 토막화가 리용되지 않았다고 가정한다.

만일 토막화가 진행되였다면 수신체계는 자료통보문을 재생할 때 매 파케트안에서 자료가 어디에 위치하고 있는가를 결정하기 위하여 편기를 리용한다. 비슷한 실례로 번호가 붙은 놀이감집짓기블로크 한조를 생각하자. 아이가 번호를 붙인 설계도에 따라 정확한 순서로 블로크들을 차례로 놓으면 그는 집도, 승용차도 지어 비행기도 만들수 있다. 사실상 아이는 자기가 무엇을 만들려고 하는지 알 필요가 없다. 그는 단순히 확정된 순차대로 블로크들을 단순히 조립하게 된다.

IP토막화편기는 같은 방식으로 동작한다. 편기는 자료통보문 앞면으로부터 얼마나 멀리 떨어 져서 포함자료들이 위치하고 있는가를 수신체계에 알려 준다. 모든것이 정상이라면 이 방식은 자료통보문을 정확한 순서대로 재결합할수 있게 한다. 길이마당은 중복이 없다는 사실과 자료가 전송과정에 틀리지 않았다는 사실을 확증검사하는 수단으로 리용된다.

실례로 자료통보문안에 토막 1과 3을 배치하고 다음 토막 2가 너무 크기때문에 3의 일부를 덧쓰게 되였다고 하면 토막 2를 배치하려고 하는 경우 문제가 있다는것을 즉시에 알수 있을것이다. 이러한 견지에서 만일 적당하게 그것들을 배렬할수 있다면 체계는 자료통보문을 알아 볼수 있게 재정렬시키려고 할것이다.

그것을 할수 없다면 수신체계는 자료를 다시 보내라는 요청을 보내게 된다.

거의 모든 IP탄창들은 중복 또는 자기 토막용으로는 매우 큰 자료라고 하여도 그것을 분할할 능력을 가지고 있다.

눈물방울공격개시

눈물방울공격은 정상크기의 자료와 0토막화편기를 가지는 표준자료파케트를 보내는것으로부터 시작한다. 눈물방울공격은 초기자료묶음을 보아서는 표준자료전송과 구별할수 없다. 그러나 다음에 오는 파케트들은 토막화편기와 길이마당을 변경시킨것이다. 이 다음의 자료흐름은 목표체계를 허물어 버리기 위한것이다.

둘째 자료묶음이 수신되였을 때 토막화편기는 자료통보문안에서 이 정보가 어디에 배렬되여야 하는가를 알려 준다. 눈물방울공격에서 둘째 파케트에 대한 편기는 이 정보가 첫째 토막안에서 그 어디든 배렬되게 된다는것을 주장한다. 자료마당이 검사되였을 때 수신체계는 이 자료가 첫째 토막의 끝을 넘어 퍼질 정도로 크지 않다는것을 알게 된다.

다른 말로 하면 이 둘째 토막은 첫째 토막을 중복하지 않는다. 즉 그안에 실제상 충분히 포함된다. 이것은 예견 못했던 오유조건이기때문에 그것을 조종할 기능이 없으며 결국 이 정보는 등록기초과 즉 수신체계의 정지를 초래한다. 어떤 조작체계의 경우에는 한개의 틀린 파케트만에 의하여 동작이 정지될수도 있다. 다른것들은 여러개의 틀린 파케트들이 수신되지 않는 한 정지되지는 않는다.

IDS 대 눈물방울

전형적인 IDS가 이 공격을 어떻게 대하는가? 눈물방울공격을 개시할 때 초기파케트전송은 표준자료전송과 같이 한다. 방금 본 이 첫 정보파케트로부터 IDS가 공격이 발생하고 있다는것을 알리는 방법은 없다.

둘째 파케트가 전송되였을 때 IDS는 자료통보문토막을 차례로 놓게 하여 이것이 눈물방울공격의 대표적인 실례의 하나라는것을 확증할수 있다. IDS는 망관리자에게 경보를 알리며 공격을 중지시키기 위한 방지수단을 만든다.

하나의 작은 문제가 있다. 만일 공격자가 한개의 틀린 파케트만으로 허물어 버리려고 하는 조작체계를 운수 좋게 찾았다면 그 공격이 발생하는것을 막는것은 너무 늦은것이다. 망관리자가 자기의 봉사기가 방금 정지되였다는것을 알게 된다는것은 사실이지만 그들은 아마 성난 사용자들의 여러번의 호출로부터도 그것을 이미 생각할것이다.

그래서 침입검출체계는 왜 봉사기가 정지되였는지는 말할수 있었지만 첫 위치에서 발생한 공격은 막을수 없었다. 앞으로 일어 나는것을 막기 위하여서는 공격자가 다시 공격하기 전에 체계를 수리하여야 한다.

그러면 왜 IP주소공격을 간단히 막지 못하는가? 공격자는 공격이 자기의 실제 IP주소가 아닌 다른 그 어떤 곳에서 온듯이 보이도록 IP속임수를 리용한다. IDS가 공격체계와 동일한 충돌구역에 있지 않다면 속임주소가 리용되고 있다는것을 발견하지 못하게 된다.

이것은 공격자가 원천IP주소를 마음대로 변경시키고 성공적인 공격을 계속할수 있다는것을 의미한다.

다른 알려 진 IDS의 제한성

1998년 2월에 Secure Networks회사는 몇개의 침입검출체계들을 검사하고 그 결과를 백서로 발표하였다. 검사결과는 공격자가 공격을 개시하여도 원만히 검출하지 못하는 많은 약점을 IDS가 가지고 있다는것을 보여 주었다.

일부 연구결과들은 좀 감상적이기는 하지만 실제 검사과정에 일부 가치 있는 문제점들을 제기하였다. 요약하면 연구는 두가지 문제에 집중된다. 즉 조작된 자료에 대한 IDS의 검출과 IDS자체에 대한 직접공격이다. 연구결과는 감시기에 기초하고 있는 침입검출이 공격을 결코 믿음직하게 검출하지 못한다는것이다.

자료조작

이 결론은 연구중에 있는 어느 한 침입검출체계들도 실제상 IP를 통하여 통신하는 체계들과 같은 방법으로 IP파케트들을 구성하지 않고 있다는 사실에 기초하고 있다. 이것은 IDS가 인식한것이 그 파케트흐름안에서 발생하고 있다는것과 수신체계는 무엇을 처리할수 있는가 하는것사이의 약간의 차이에 기인한다.

한가지 문제는 일부 침입검출체계들이 IP머리부와 검사합마당이 동일한가를 확인하지 않는다는것이다(그림 8-1을 참조하기 바란다.). 이것은 수신체계에 의하여 반드시 수행되여야 하며 이 마당조작은 IDS로 하여금 수신체계가 처리하는것과는 다른 자료를 기

록하도록 한다.

연구에 리용한 실례는 PHF CGI공격이였다. IDS는 모든 HTTP요청을 구성하고 있는 자료부분안에서 문자렬 phf를 찾는 방법으로 이 공격을 알아 낸다. 이 모형이 검출되였다면 IDS는 공격이 일어 났다고 간주한다. 숙련된 공격자는 렬 phoof를 만드는 매개의 문자를 파케트렬로 보내려고 시도할수 있다. 그 공격자는 검사합마당을 조사하여 문자 0를 포함하고 있는 매개 묶음이 실패검사합을 가지게 한다. 수신체계(검사합을 확증해야 하는)가 문자렬 phf를 처리하는 동안 IDS(검사합을 확증하지 않는)는 이 전송을 phoof로 읽어 들인다.

자료흐름이 어떻게 처리되는가 하는데서의 이러한 차이가 분명히 큰 문제로 되지만 그것은 극복할수 있다. 실례로 이 문제를 공개한 하나의 제품인 ISS RealSecure에서 그것은 다음 제품들에서 수정되였다.

이러한 문제들은 첫 개발기술분야에서 전형적으로 제기된다. 방화벽개발자들은 류사한 연구과정을 거쳐 왔으며 오늘날에도 계속 개량해 나가고 있다. 망보안이 여전히 침체된 분야로 될것이라고 주장할 근거는 없다.

IDS에 대항한 공격

Secure Networks가 연구하여 발표한 다른 문제는 직접공격에 대한 IDS의 약점이였다. IDS에 대항한 직접공격은 침입을 검출할 능력을 억제할수 있기때문에 하나의 문제로 된다. IDS를 중지시킴으로써 공격자는 발견될 근심이 없이 망에 대항하여 공격을 개시할수 있다.

IDS 대 방화벽

여기서는 방화벽과 IDS사이의 중요한 차이를 강조한다. 방화벽은 주변감시수단으로 작용한다. 이것은 모든 자료흐름이 망의 한 구역에서 다른쪽으로 이동하기 위하여서는 방화벽을 통과하여야 한다는것을 의미한다. 방화벽이 공격 당하고 봉사기들이 파괴된다면 자료흐름을 통과시킬수 없게 되였다는것을 의미하는 전형적인 틀린 열기현상이 나타나게 된다. 이것은 모든 전송을 마비시키지만 방화벽을 무력하게 만들고 내부호스트에 대한 공격을 개시할 기회를 노리는 공격자들을 방해한다.

한편 어떤 IDS는 망토막들사이에 위치하지 않는다. 그런것은 하나의 충돌령역안에서 동작하도록 설계되였다. 만일 IDS가 무력하다면 자료흐름이 정지되지 않기때문에 기술적으로 틀린 닫기로 된다. 망자원들에 접근하는 동안 공격자는 IDS가 정지되게 할수 있다. 그것은 IDS가 비직결인 조건에서 개시된 모든 공격들이 문서화되지 않는다는것을 의미한다.

다시금 이 문제는 Secure Network의 연구가 서술한것처럼 그렇게 극복할수 없는것은 아니다. 매개 망호스트에 의하여 직접 주소화할수 있는 침입검출체계를 가져야 할 합법적인 리유는 없다. 망자료흐름을 알아 내는 작용은 유효 IP주소를 요구하지 않는

다. 련결을 요구하는 체계들은 다음의것들만이다.

- 수감기
- 조종탁
- DNS체계(IP주소들을 호스트이름으로 변환하려고 하는 경우)
- 방화벽 또는 경로기(IDS가 려파규칙을 변경시킬것을 요구하는 경우)

공공망에서 IDS통신을 분리하는것은 사설 IP주소공간에 따라 분리된 사설망을 리용하는 방법으로 쉽게 실현할수 있다. 사실상 이 부분망에 대한 경로조종을 무시한다면 그것은 지역별로 수행될수 있다. 수감기는 IP규약탄창을 요구하고 기본망에 대한 IP주소를 요구하지만 이 주소는 합법적인것이 아니라도 된다. 이러한 구성실례를 그림 8-2에서 보여 주었다.

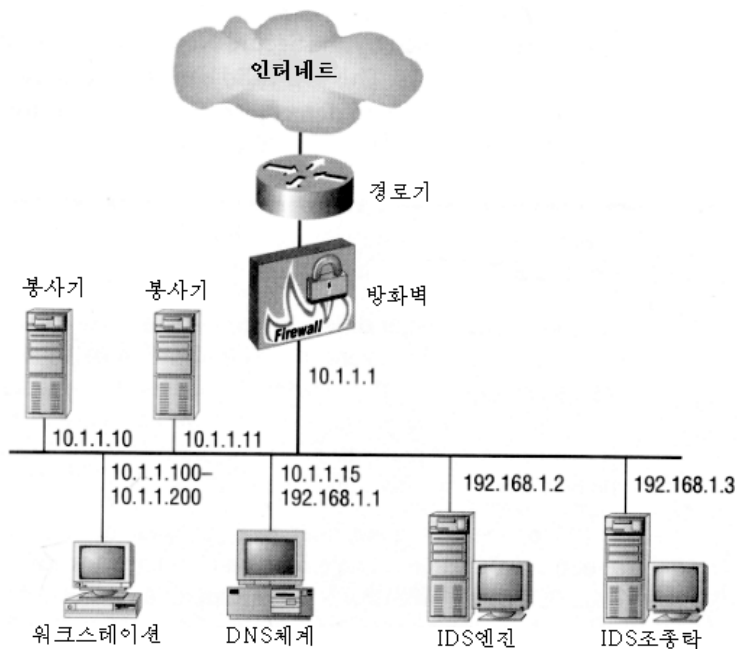



그림 8-2. 개별부분망을 통한 IDS관리

그림 8-2에서는 정규적인 망체계들에 10.1.1.0 부분망으로부터 주소공간이 할당되였다. 이 부분망안에 있는 모든 체계들은 어떤 인터네트접근준위를 허락 받는다. 그리고 방화벽은 이 주소들을 가지고 NAT를 리용하도록 구성된다. 방화벽이 관계하는 범위에는 10.1.1.0 망만이 있게 된다.

그것을 세밀히 살펴 본다면 DNS체계가 2개의 IP주소 즉 하나는 10.1.1.0 망에 관한것이고 다른 하나는 192.168.1.0 망에 관한것을 가지고 있다. 이 장치는 그 두 부분망사이에서 자료흐름이 경로조종되지 않도록 특수하게 구성되여 있다. IP전송이 정지된다면 두 부분망우의 체계들은 통신이 가능하지만 그것은 경로기로서 작용할수 없고 그것들

사이에서 자료흐름을 전송할수 없다.

IDS수감기와 감시기들은 192.168.1.0 부분망에 관한 주소공간을 사용하고 있다. 그것들이 각각 DNS체계와 송신을 하는 경우 10.1.1.0 주소를 리용하는 그 어떤 체계와도 통신이 불가능하게 된다. 이것은 두 망토막사이에 경로를 조종하는 장치가 없기때문이다. IDS역시 방화벽밖에서 체계들로부터 임의의 자료를 주고받는것이 불가능하게 된다.

IDS가 자료흐름을 감시하려고 할 때 무엇이 발생하는가? 언급한바와 같이 IDS수감기는 자기 자체의 부분망우의 자료흐름만이 아니라 망우에서 모든 자료흐름을 포착하게 된다. 이것은 10.1.1.0 부분망우의 체계들과 인터네트사이의 통신을 포함하여 국부망우의 모든 자료흐름을 기록하는것이 완전히 가능하다는것을 의미한다. 이러한 발견은 192.168.1.0 부분망을 통하여 조종탁에 보고될수 있다.

둘중 어느 한 체계가 IP주소를 호스트이름으로 변환하려고 할 때 무엇이 발생하는가? DNS체계는 정보를 경로조종할수는 없다. 이것이 사실이라면 주소문의를 해결하기 위한 대리자로서 DNS체계를 리용할수 있다는것을 의미한다.

제3장에서 DNS가 단순히 호스트이름들을 IP주소들로 또한 그 반대로 바꿀 의무가 있는 하나의 응용층봉사라는것을 보았다. 수감기가 DNS질문을 DNS봉사기에 보낼 때에는 국부적으로 축적된 정보로서 요청을 응답하려고 해도 된다(국부구역파일들을 통하여서든지 혹은 완충된 입구점들을 통하여서든지). 만일 이것이 불가능하다면 DNS봉사기는 뿌리이름봉사기들중의 하나와 접촉하려고 할것이다.

뿌리이름봉사기에 대한 제일 좋은 경로가 10.1.1.15 IP주소를 거치도록 구성되였다면 방화벽에 10.1.1.1로 지적한 표준경로를 만드는것처럼 DNS봉사기는 원천 IP주소 10.1.1.15 를 리용하여 요청을 전달하게 된다. DNS봉사기는 질문을 경로조종하는것이 아니고 질문을 풀기 위한 대리자로서 작용하는것이다.

질문에 대한 대답을 받을 때 DNS봉사기는 자기가 알고 있는 제일 좋은 경로를 리용하여 수감기에로 응답을 되돌려 보낸다. 이것은 체계가 192.168.1.1 주소를 리용하여 전송을 진행하여야 한다는것을 말한다. 다시는 정보에 대한 경로선택을 하지 않고 DNS장치로서 그것을 대용한다. 이것은 IDS가 나머지 망과 같은 부분망주소를 리용함이 없이 DNS질문들을 완전히 해결할수 있다는것을 의미한다.

결과 인터네트로부터 직접 주소화할수 없는 하나의 숨겨 진 부분망이 얻어 진다. 공격자는 IDS수감기나 조종탁에 접속하기 위하여서는 방화벽을 뚫고 들어 가거나 DNS봉사기를 파괴하여야 한다. IDS가 직접 주소화될수 없다면 명백히 공격을 할수 없다.

일러두기

방화벽과 마찬가지로 공공망에서 IP를 리용하고 있는 IDS수감기는 리용에 앞서 보강되여야 한다. 여기에는 그것이 최근의 보안관련수정프로그람들을 모두 가지고 있도록 하는것과 함께 그 체계에 불필요한 봉사들은 어느것도 동작시키지 않는다는 담보를 포함하고 있다. 보강된 체계는 공격을 더 잘 막게 되며 따라서 안전감시처리를 하는데 가장 좋은 플래트홈으로 된다.

IDS의 보복수단

침입검출체계는 경과등록 및 경보를 하는것과 함께 그 처리에서 다른 두가지 능동보복수단들을 가지고 있다.

- 대화중지
- 려과규칙조작

이것들은 매개 전문적인 제품에 따라 다른데 매 방법의 일반적능력과 약점을 살펴보기로 하자.

IDS에 대한 내부공격

IDS수감기와 조종탁들은 내부공격에 취약하다. 10.1.1.0 망우에서 그 누군가가 IDS의 IP주소를 발견한다면 192.168.1.0 부분망에 대하여 이 체계를 직접 주소화하기 위하여 국부주소를 변화시키거나 속이는것은 쉽다. 이것을 《애매성을 통한 안전》이라고 하는데 체계는 그것이 어디에 숨겨 져 있는지 모르는 동안만 안전하다 더우기 이러한 체계들을 인터네트로부터 완전히 접근할수 없게 만듦으로써 가능한 공격시점의 령역을 매우 제한하며 공격자를 발견하는 과정을 쉬워 지게 한다.

내부공격들이 문제라면 IP탄창을 요구하지 않는 IDS를 쓸수 있다. 실례로 Real Secure는 감시되는 망에 속한 IP를 가지고 있지 않는 체계로부터의 망감시를 지원한다. IP주소가 없으면 체계는 IP에 기초한 어떠한 공격에 대하여서도 영향을 받지 않는다. 물론 이것 역시 조종탁을 감시하기 위한 전문적인 고찰을 하여야 한다는것을 의미한다. 수감기와 같은 체계에 대한 IDS조종탁을 가동시키거나 혹은 수감기에 둘째 망기판을 설치하여야 하는데 그래야 개인부분망을 통하여 조종탁을 기지고 통신을 할수 있다.

대화중지

대화중지는 실현하기 제일 쉬운 보복수단이다. 그것을 실현하기 위한 몇가지 방안들이 있지만 제일 기초적인 형태로서의 대화중지는 IDS를 재설정하거나 공격대화의 매개 끝을 막는 방법으로 만들어 진다. 이것은 앞으로의 공격개시로부터 공격자를 막을수는 없지만 현존대화가 진행되는 동안 어떤 그이상의 손실을 일으키는 공격자는 막는다.

실례로 IDS수감기가 FTP대화동안에 문자렬 CWD ~root를 보내려고 하는 공격자를 발견한다고 하자. 정확히 수행하였다면 이러한 공격은 공격자에게 뿌리준위 FTP로서 일부 이전 체계들에 접근하도록 한다. 이러한 접근준위는 아무런 통과인증없이 허락되며 공격자는 체계상의 임의의 파일에 읽기쓰기를 할수 있다.

대화중지가 가능하다면 IDS수감기는 먼저 식별하고 이 잠재공격을 기입하며 다음에 련결을 억지로 잡아 떼기 위하여 대화량쪽에 거짓 ACK-FIN파케트들을 보낸다. IDS수감

기는 련결의 다른끝에 있는 체계인듯이 가장하면서 이것을 실행한다. 실례로 원천 IP주소, 포구번호, FTP봉사기의 순서번호를 리용하여 공격자에게 ACK-FIN을 전송한다. 이것은 공격자가 파일체계에 접근하는것을 막으면서 통신대화를 효과적으로 차단하게 한다. 사용에서는 IDS수감기에 따라 무한히 혹은 사용자가 설정한 시간주기동안 공격호스트로부터 모든 통신을 차단해도 된다.

대화중지가 강력한 특성이기는 하지만 제한성이 없는것은 아니다. 실례로 이 장의 앞에서 이미 서술한 눈물방울에 대한 실례는 침입검출체계가 공격을 막을수 없다는것을 보여 주었다. FTP공격에 반응할만큼의 충분한 시간을 IDS가 가지고 있다고 하여도 한개의 틀린 IP머리부만으로 체계를 충분히 파괴할수 있다면 눈물방울로부터 체계를 보호할정도의 속도로 충분히 빨리 반응하기는 어렵다.

려과규칙조작

일부 IDS수감기들은 계속되는 공격을 막기 위하여 경로기나 방화벽의 려과규칙들을 변경시킬수 있는 능력을 가지고 있다. 이것은 목표호스트에 추가적인 자료흐름을 보내는 공격체계를 중단시킨다. 즉 IDS는 협의자 IP주소로부터 들어 오는 모든 자료흐름을 차단하는 새로운 려과규칙을 방화벽에 첨부한다. 려과규칙조작이 강력한 하나의 새 창안품이기는 하지만 그런데도 제한성이 없는것은 아니다. 이 특성의 의미를 충분히 파악한 다음에야 그것을 리해할수가 있다.

긍정적면에서 보면 려과규칙조작은 대화중지보다는 매우 적은 망자료흐름을 가지고 공격을 막을수 있다. IDS가 일단 려과규칙들을 변경시키면 공격자료흐름은 멈춘다. 대화중지에서 IDS는 매 공격대화를 련속적으로 막아야 한다. 만일 지속적공격을 한다면 이것은 선로에 통신량이 아주 많아 지게 할수 있다.

부정적면에서 보면 려과규칙조작은 항상 100% 효과적이 아니라는것이다. 실례로 방화벽안에서 공격원천 IP주소는 무엇인가? 이 경우에 려과규칙을 변경시키는것은 효과가 없다. 공격자료흐름은 실제상 방화벽을 결코 통과하지 못하기때문에 려과규칙들의 지배를 받지 않는다. 이것은 려과기교체가 공격에 영향을 미치지 않는다는것을 의미한다.

숙련된 공격자는 실제주소보다는 오히려 속임IP주소를 사용할수 있다. 방화벽이 초기공격을 차단시킬수도 있지만 공격자가 하여야 할 일은 이 새로운 규칙변경을 우회하기 위하여 또 하나의 속임주소를 선택하는것이다. 대화중지에서 IDS는 원천IP주소가 아니라 공격징후에 기초하여 반작용한다. 이것은 려과규칙조작으로는 못하지만 대화중지는 련속적으로 공격을 막아 낼수 있다는것을 의미한다. IDS는 성공적인 규칙변화를 일으키며 발견된 모든 속임주소들을 차단할수 있다. 그러나 공격자가 원천IP주소를 빨리 변화시킨다면 IDS는 유지할수 없게 된다. 려과기를 변경시키기 위하여서는 IDS와 방화벽이 일정한 시간동안(대체로 10～30초) 기다려야 한다.

경 고

현존 려과기규칙을 변경시킬 능력이 DoS공격에 대하여서도 개발되였다. 공격자가 다중려과기규칙변화를 련달아 일으키기 위하여 원천IP주소를 일부러 변화시킨다면 방화벽은 바빠서 자료흐름통과를 중단시키게 된다. 려과기규칙이 변하는 동안에는 어떤 능동대화도 물론 종결되게 된다.

명백히 려과기규칙들을 변경시킬 능력은 아주 유해로운것으로 간주되는 그러한 공격들에 대하여서만 좀 리용된다. 실례로 1996년이전에 나온 모든 종전의 IP장치와 체계는 죽음의 Ping에 대하여 취약하다. 죽음의 Ping이란 너무 큰 ICMP자료통보문을 보냄으로써 목표체계에 대한 IP통신규약탄창을 파괴하는 하나의 수단이다. 종전의 낡은 체계들을 가지고 환경을 구축한다면 이러한 공격들을 막기 위하여 려과기규칙들을 변경시키는것은 효과가 적다. 빈번한 규칙변화가 잠정적으로는 봉사거부의 원인으로 되지만 이러한 자료흐름을 통과하게 하는것은 모든 IP통신을 거의 중단시킨다.

일러두기

죽음의 Ping은 망하드웨어뿐만 아니라 콤퓨터체계들에도 영향을 미친다. 모든 IP장치들이 이러한 형태의 공격에 대항하여 보강되였는가를 확인하여야 한다.

주 의

모든 침입검출체계들이 모든 방화벽과 경로기들에 적용가능한것은 아니다. 실례로 ISS RealSecure는 Check Point 방화벽-1만을 변경시킬수 있다. 현재 특성발표문에 Cisco경로기들을 추가시킬 계획이 있다고 하지만 그것은 어떤 다른 방화벽제품과 호환되지 않는다. 그래서 대화중지가 이러한 특성을 지원하고 있는 어떤 IDS에 의하여 리용될수 있는데 방화벽기능을 수행하는 적당한 체계를 리용한다면 려과조작만을 할수 있다.

호스트기초IDS

지금까지는 모든 망자료흐름을 통과시키는 전용의 봉사기와 감시기에서 동작하는 침입검출체계들을 주로 보았다. 이 장치들은 전체 충돌령역안에서 자료흐름을 조종하는데 리용되고 있다. 그러나 단일체계만을 보호하기 위하여 설계된 호스트기초IDS제품들이 있다.

호스트기초IDS는 비루스주사장치와 류사하게 작용한다. 그것의 쏘프트웨어는 보호하려는 체계상에서 배경처리로서 돌아 가면서 이상작용을 검출하게 된다. 이상작용에는 HTTP요청을 통하여 미지의 지령들을 보내려는 시도나 파일체계변경 등이 포함된다. 이상작용이 검출되였을 때 IDS는 공격하는 대화를 중지시키고 체계의 기본관리자에게 경보를 보낼수 있다.

몇가지 결함들

호스트형침입검출체계들은 몇가지 결함들을 가지고 있는데 그것으로 하여 여러 환경들에서 그것이 비실용적인것으로 되고 있다. 초기의 제품들은 대부분 특정형식의 체계만을 감시할수 있었다. 실례로 NetWork Associate가 만든 CyberCopServer는 Web봉사기들을 보호할 능력만 있다. 만일 그 봉사기가 여러가지 봉사(DNS, 파일공유, POP3 등)를 하고 있다면 호스트기초IDS체계는 침입검출능력이 없을수 있다.

IDS의 대다수가 사용자접근권변경과 같은 핵심봉사기능들을 감시하는 동안 공격자는 체계를 변화시킬 시도에 앞서 IDS를 무맥하게 할 방도를 찾는다. IDS가 무맥하게 되였다면 공격자는 체계를 자유롭게 파괴한다.

다른 문제는 호스트형침입검출체계들이 단순히 배경처리로써 가동하며 체계의 핵심통신기능에 접근하지 않는다는것이다. 이것은 IDS가 통신규약탄창 그자체에 대항한 공격을 막을 능력이 없다는것을 의미한다. 실례로 장비가 약한 NT봉사기를 파괴하기 위하여서는 10개정도의 눈물방울파케트를 리용하면 된다. 이것은 망에 기초한 IDS가 반작용하고 보복수단을 취하는데는 충분한 시간이지만 호스트기초IDS는 무력하게 남아 있게 된다. 왜냐하면 이 자료흐름을 전혀 알지 못하기때문이다.

보호하려는 체계상에서 침입검출프로그람을 돌리는데는 론리적인 계산오유가 있다는것을 역시 론의할수 있다. 공격자가 체계에 침투할수 있다면 공격자는 더우기 IDS를 위태롭게 한다. 이것은 아주 나쁜 일이다. 즉 공격자는 최종보안보호선에 구멍을 내게 된다.

일러두기

햇내기공격자들만이 경과기록이라든가 의심 받을수 있는 처리를 깨끗이 하지 못하여 자기의 흔적을 없애지 못한다. 이것이 체계관리자들로 하여금 모든 경과기록목록을 원격체계에 발송할것을 많은 보안전문가들이 권고하고 있는 리유이다. 그 체계가 공격자때문에 위태롭다면 경과기록들은 경보를 기록할수 없다. 이와 같은 원리가 역시 침입검출체계들에 확장될수 있다.

언제 호스트기초IDS가 효과적인가?

이 모든 결함에도 불구하고 호스트형침입검출체계들은 자기의 위치를 차지한다. 실례로 보호하려는 Web봉사기가 DMZ망토막우에 위치하고 있다고 가정하자. 이 DMZ는 방화벽뒤에 있지만 Web봉사기만을 포함하는 토막과 분리된 상태에 있다. 방화벽은 HTTP로 Web봉사기에로의 자료흐름만 허락하도록 구성되여 있다.

이러한 경우에 호스트기초IDS제품은 Web봉사기를 보호하는데 충분하다. 그것은 방화벽이 대부분의 보호를 제공해 주기때문이다. 방화벽은 Web봉사기로 할수 있는 자료흐름이 오직 HTTP요청뿐이라는것을 확인하게 된다. 이것은 Web봉사기상에서 돌아가는 다른 모든 봉사기들에 대하여 걱정을 안해도 된다는것을 의미한다.

호스트형침입검출체계는 의심스러운 파일접근요청이라든가 CGI와 Java리용이 이러한 HTTP요청속에 포함되여 있지 않으며 체계상에서 돌아 가는 Web봉사기에로 통과되지 않는다는것만을 담보하여야 한다. 이것은 비록 적지 않은 공적이지만 IDS가 조종할것을 기대하였던 각종 리용범위를 제한한다.

호스트기초IDS는 완전교환환경에서 매우 유익할수 있다. 이것에 대하여서도 론의되고 있다(그림 8-3).이 그림에서 모든 체계들은 교환기에 직접 련결된다. 실제상 이것은 매개 체계에 그자신의 충돌구역을 가져다 준다. 즉 교환기가 통신에 참가한 두 체계만이 자료흐름을 볼수 있도록 모든 단일자료흐름을 분리시킨다.

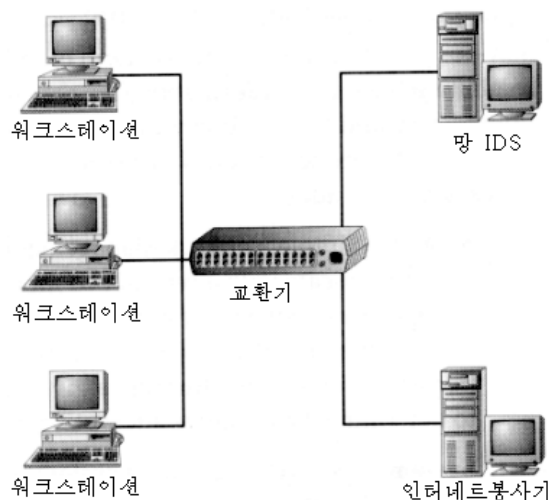



그림 8-3. 망중심

교환기가 통신대화를 분리시키기때문에 망에 기초한 IDS는 모든 통과하는 망자료흐름을 알수 없게 된다. 만일 작업국이 인트라네트Web봉사기에 대항하여 공격을 개시한다면 IDS는 공격이 진행되고 있으며 그래서 보복수단을 취하기 곤난하다는것을 완전히 알아 차리지 못하게 된다. 뿐만아니라 이것은 공격이 IDS경과기록에 나타나지 않고 사건기록도 되지 않는다는것을 의미한다.

호스트기초IDS는 인트라네트 Web봉사기를 보호하는데 제일 유리할수 있다. 이것은 보호하려는 체계상에서 돌아 가기때문에 교환기의 자료흐름분리속성의 영향을 받지 않는다. Web봉사기가 살피고 있는 모든 자료흐름을 알기때문에 HTTP에 기초한 공격으로부터 체계를 보호할수 있게 한다.

일러두기

대부분의 교환기개발자들은 감시포구로서 한개의 교환기포구를 구성하도록 한다. 이것은 이 포구에 련결된 임의의 체계에로 보내는 모든 자료흐름을 교환기가 복사전송할수 있게 하여 준다. 만일 교환기환경에서 망중심 IDS를 사용하려고 한다면 IDS가 모든 통과자료흐름을 확인할수 있다는것을 확인하기 위하여 이 감시포구에 그것을 련결시키면 된다.

IDS융합

전통적인 IDS의 제한성을 극복할뿐만아니라 보다 혁신적인 보안을 하려는 시도에서 IDS연구는 자료의 통합방향으로 혹은 조사적인 견지에서 볼 때 아주 일반적인 술어인 융합이라는 말을 써서 추진되고 있다. 다른 형태의 정보들과 원천들을 봉사기들과 콤퓨터들에서 나오는 파케트정보(실제로 통신되는 정보)와 결합함으로써 IDS체계들은 보다 더 정확하게 공격에 대한 정보를 결정할수 있다.

추가적인 자료원천들은 다음의것들을 포함한다.

SNMP(단순망관리규약) 이것은 집중감시체계를 가지고 망장치들이 통신하도록 하며 무슨 자료가 전달되고 있는가가 아니라 어떻게 작용하고 있는가를 보고한다. 주어 진 대면부를 통하여 통과하는 초당 자료흐름량이 많은 망감시체계를 현대화하는 경로기가 바로 그 하나의 실례로 된다(대면부는 해커가 DoS공격을 시도할 때 IDS에 의하여 결정하기 위하여 리용될수 있다.).

체계경과기록(System logs) 거의 모든 조작체계들은 임의의 주어 진 시각에 자기의 총적상태와 관련한 폭 넓은 상세한 자료를 기록하도록 구성될수 있다. 이때 매개 조작체계성분으로부터 발생하는 이상자료도 기록할수 있다. 전자우편의 도착시간이 아니라 원본봉사기의 IP주소를 기록하는 전자우편봉사기를 고찰하기로 하자. 이 통보는 비루스를 운반하는 전자우편경로를 추적하며 피해를 입은 봉사기로부터 발생하는 임의의 전자우편을 려과하도록 체계안의 모든 전자우편봉사기들에게 알리기 위하여 IDS를 사용할수 있다.

체계통보(System message) 거의 모든 적절한 체계자료는 보통 기록되는데 이것은 틀린 자료의 결합이거나 또는 단순히 조작체계결함일 때에는 그렇게 되지 않는다. IDS는 체계통보들을 리용하여 전체 망에 대한 보다 큰 표상을 만들며 이것은 망상태로부터 나오는 자료(융합)와 회복의미(패턴분석)를 결합하게 한다.

명령들(Commands) 거의 모든 조작체계들은 모든 사용자들이 공포한 매개 단일명령을 기록하기 위하여 설계 또는 구성되는것이 아니다. IDS융합은 바로 그러한 제한성을 극복하기 위하여 설계되였다. 즉 체계가 자기자신을 기입하는 방법으로 놓친 패턴들을 해명한다(이것은 직접 체계나 또는 보안특성에 대한 정보를 보고만 한다.). 독점적인 회사정보를 지워 버리기 위하여 설계된 명령이 하나의 실례로 된다. 통보는 회사에 극단적인 손해를 주지만 체계의 완전성을 파괴하거나 영향을 미치지는 않는다.

사용자행위(User Behavior) 사용자명령이나 시간에 따르는 일상적인 사용자행위를 감시한 결과는 자기자체의 패턴을 만들며 사용자구좌활동을 부단히 해석함으로써 IDS는 어떤 더 큰 위반이나 체계에 대한 침투가 일어 나기전에 그 구좌가 습격을 받았는가를 결정할수 있다.

사용자, 체계, 망자료와 행위모두를 해석한다는 개념은 아주 쉬운것처럼 생각되지만 실제로 IDS융합은 아주 어렵다고 본다. 그것은 복잡한 수학공식에 의거하며 일부 강한 후비원천들이 효과적으로 동작할것을 요구한다. 이것은 아직 주관적이며 실험적으로나 진행되고 있다. 그럼에도 불구하고 IDS융합은 협동자료공유와 공격을 받은 모든 망들에 대한 응답을 통하여 망보호를 개혁하도록 해준다.

IDS의 설치

IDS를 설치하는 방법을 고찰하기 위하여 인터네트보안체계(ISS) Real Secure를 살펴보기로 하자. RealSecure수감기는 실제상 여러개의 제품들로 구성되여 있다.

RealSecure 조종탁(작업그룹관리자)은 망과 봉사기수감기들 모두를 포함하여 전체 RealSecure체계를 조종한다. 또한 주자료기지를 장비한다(이것은 보고서를 작성하는데 리용된다.).

RealSecure 망수감기는 주어 진 토막에서 모든 망자료흐름을 기록하며 그것을 공격징후와 비교한다.

RealSecure 봉사기(OS)수감기는 특정의 체계를 지향한 공격에 대하여 체계워크스테이션록들과 대면부자료흐름을 감시한다.

시작하기전에

이 부분에서는 RealSecure의 Windows NT판을 기본으로 고찰한다. 언급된바와 같이 같은 체계 혹은 서로 다른 플래트홈들상에서 수감기들과 조종탁이 가동하도록 선택할수 있다(이 경우에 비록 망과 봉사기조작체계수감기들을 둘다 동시에 같은 플래트홈에서 가동시킬수 없을수도 있다.). 이것을 결정하는 인자들은 비용, 성능 그리고 교환기망을 가동시키는가 하는것들이다. RealSecure 쏘프트웨어에서는 리용하려는 플래트홈이 하나이든 둘이든 들어 가는 비용은 같다. 그러나 두개의 플래트홈인 경우에 명백히 Windows NT 봉사기사용허가와 두개의 봉사기급의 체계를 구입하여야 한다.

만일 체계가 낮은 대역너비련결을 감시하게 된다면(T1속도 혹은 그이하) 질 낮은 두개의 콤퓨터보다는 차라리 한개의 《강력한》기계를 가동시키는것이 아마 더 낫다. 만일 중추망이나 다른 고자료흐름구역을 감시할 계획이라면 두개의 적절히 장비된 체계들을 구입하는 문제를 고려해 볼수도 있다. 수신하고 처리하는 선로상의 매개 파케트는 CPU능력이 크다. Real Secure는 130개이상의 서로 다른 이상조건에 대한 매개 파케트를 검사한다. 요구된다면 기록일지의 기입과 보복수단의 적용을 결합시키면 아주 만가동하는 체계를 얻게 된다.

IDS를 어디에 설치하겠는가?

IDS를 어디에 설치하여야 제일 좋은가를 결정하기 위하여서는 《어느 체계를 보호하려고 하며 어느 원천으로부터 보호하여야 하는가》에 대한 질문으로 제기하여야 한다. 미리 이러한 관점을 명백히 하는것이 좋다. 실제적으로는 1개이상의 IDS수감기가 요구된다는것을 알아야 한다. 하드웨어나 쏘프트웨어를 구입하기 위한 요청서를 작성하기에 앞서 마음속으로 가장 견고한 보안대책을 가지고 있어야 한다.

하나의 위치배비도를 그림 8-4에 보여 주었다.

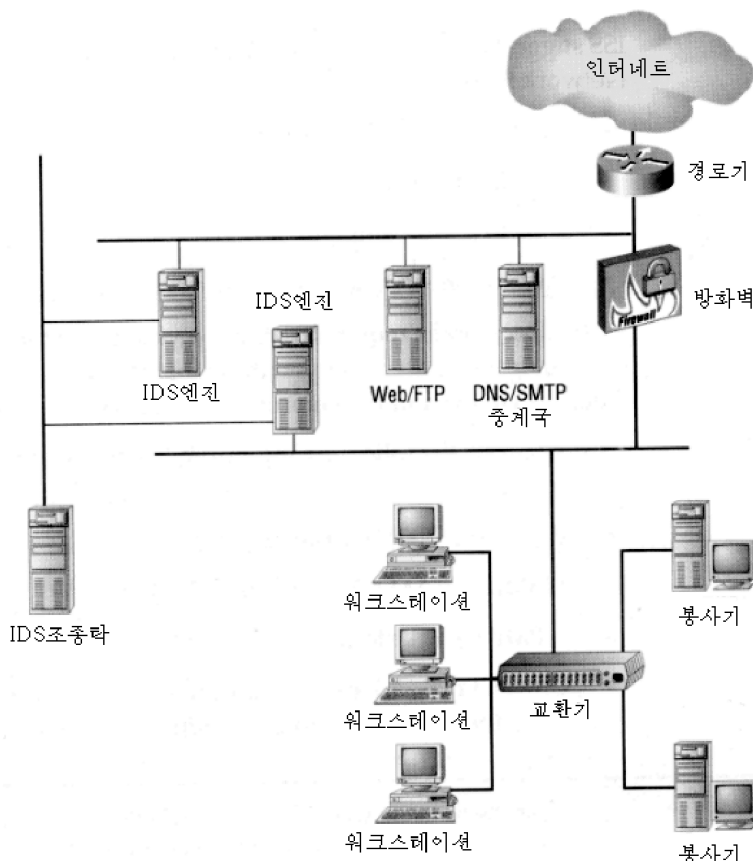



그림 8-4. IDS수감기 2개를 쓰는 위치배비도

이 모형에서 DMZ와 방화벽내부접속은 둘다 감시를 받고 있다. 이것은 인터네트로부터 모든 귀환자료흐름을 확증할수 있게 한다. 또한 현존방화벽을 강화할수 있게 한다. IDS수감기들은 둘다 공공의 망토막에 속하는 IP가 없이 가동하고 있다. IP는 조종탁뒤에 수감기를 련결하는 망기판상에서만 가동하고 있다. 이것은 IDS수감기들이 공공망토막상의 모든 체계들에서 완전히 보이지 않도록 하여 준다.

그러나 이렇게 구성하여도 몇가지 제한성이 있다. 우선 방화벽에서 목표로 삼은 인터네트로부터의 공격자료흐름을 감시할수 없게 되는것이다. 방화벽이 그러한 활동을 기록할수 있다고 하여도 불충분한 파케트획득, 동적려파규칙조작 또는 IDS가 제공할수 있는 일부 다른 특성에 대하여 리득이 없을수 있다. 인터네트련결이 T1 혹은 그보다 작고 그리고 인터네트자료흐름을 감시만 하려고 한다면 실제로 좋은 한개의 봉사기를 리용하여 방화벽밖에서 모든 IDS기능들이 동작하게 하는것이 더 좋을수 있다. IP가 이러한 체계에서는 필요없기때문에 공격으로부터 안전하게 된다.

그림 8-4에 보여 준 설계안이 가지고 있는 다른 제한성은 내부체계들사이에서 발생하는 자료흐름을 감시할수 없게 한다는것이다. 모든 망자료흐름을 감시하는것이

목적이라면 교환기상에서 자기의 포구에 내부 IDS수감기를 이동하여도 좋으며 이 교환기포구를 형성하여도 좋다. 이것은 방화벽안에서 모든 자료흐름활동을 알게 하여준다.

가능한만큼 망에 열쇠를 채우는것이 목적이라면 다음과 같은 해결책들을 결합하는것이 좋다. 즉 한개의 IDS수감기를 방화벽밖에 설치하고 다른 IDS수감기는 교환기포구감시밖에 두는것과 두개의 수감기들을 가지고 사설부분망을 통하여 조종탁으로서 통신하는것이다. 이것은 중앙조종탁으로부터 여전히 조종을 감시하는 동안 망안에서 모든 통과자료흐름을 감시할수 있게 하여 준다.

일단 감시하려는 구역이 선택되였으면 적당한 하드웨어뿐아니라 요구되는 IDS수감기들도 몇개 선택할수 있다.

하드웨어에 대한 요구사항

ISS는 RealSecure NetWork Sensor에 관하여 다음과 같은 하드웨어에 대한 최소한의 요구사항을 제기하고 있다.

- 펜티움Ⅱ 300MHz처리기
- 128MB RAM
- 110MB 디스크기억
- 최소한 한개의 PIC 망기판

디스크기억요구사항은 대체로 높지 않다. 대량자료흐름구역을 감시하려고 하거나 원천자료를 많이 획득하려고 생각한다면 많은 디스크공간을 확장할것을 계획하여야 한다. ISS는 RealSecure 조종탁에 대하여서는 다음과 같은 하드웨어에 대한 최소한의 요구사항들을 제기하고 있다.

- 펜티움Ⅱ 300MHz 처리기
- 128MB의 RAM(256MB를 권고한다.)
- 수감기당 100MB디스크기억
- 하나의 PIC망기판(추가적인 NIC는 원격기계상의 수감기들과 통신하기 위한 안전한 망을 구성하는데 리용될수 있다.)

일러두기

디스크공간은 크게 하는것이 좋다. 부족되는것보다는 많은것이 더 좋다. 더 많은 디스크공간을 리용할수록 더 오래 경과기록을 보유하게 된다. 이것은 오랜 기간의 정황을 살펴 볼 때 아주 중요하다. 같은 체계상에서 수감기와 조종탁을 가동시키려고 한다면 처리기요구를 400MHz 펜티움Ⅱ와 기억요구를 192MB까지 높이는것을 고려하여야 한다.

NT의 설치

RealSecure는 IDS기능을 보장하는 Windows NT상에서 가동하게 된다.
NT봉사기를 설치할 때 다음과 같은 차림표지시를 준수하여야 한다.

- NT를 구성하기전에 모든 필요한 망기판들을 설치하시오.
- NT조작체계와 교체파일을 적재할수 있게 800MB의 NTFS C분할을 만드시오.
- IDS프로그람파일과 경과기록들을 적재하기 위한 나머지 구동기공간(최소 200MB)의 NTFS D분할을 만드시오.
- TCP/IP를 제외한 모든 규약들을 제거하시오.
- 조종탁에서 봉사기대화칸을 열고 Event Log봉사와 Net Logon봉사를 제외한 모든 봉사를 무시하시오.
- 봉사 Pack 5(또는 그이상)의 128bit판을 설치하시오.
- 최소한 getadmin-fix, ndis-fix, pent-fix, srvr-fix 와 teardrop2-fix를 설치하시오. scsi-fix와 같은 다른것들은 요구에 따라 설치할수도 있다.
- System Properties의 Performance칸에서 전경응용프로그람 Boost를 None으로 변경시키시오.
- 봉사기봉사가 가동하고 있다면 봉사기특성대화칸으로 넘어 가서 망응용을 위하여 Optimization을 Maximize로 변화시키시오.

일단 이 사항들을 수행하면 비상회복디스크를 만들고 RealSecure를 설치할 준비가 된것으로 된다.

RealSecure설치

RealSecure설치는 매우 쉽다. 만일 전자우편을 통하여 ISS와 접촉한다면 여러가지 설치파일데모를 내리적재할수 있다. 데모는 15일간에 만기되는 웅근제품을 단순히 복사한것이다. 보다 더 많은 정보를 얻기 위하여서는 ISS Web싸이트 www.iss.net를 보시오.

설치에서 첫 요소는 RealSecure Workgroup Manager(조종탁)이다. 자체추출실행은 림시등록부에 일부 파일들을 복사하고 Setup프로그람을 시동시키는것으로부터 시작한다. 적어도 Service Pack 5가 설치되지 않았다면 Setup프로그람은 경보를 내고 실행을 중지한다.

그림 8-5에서 보여 준바와 같이 설치하려는 프로그람의 어느 부분을 선택할것인가를 먼저 묻게 된다.

조종탁설치, 개인열쇠의 재적재, 조종탁의 공개열쇠배송 등을 선택할수 있다. 망이든 OS/Server수감기들이든 설치는 절차를 서로 따로 가지고 있다. 뒤의 두개 선택은 IDS쏘프트웨어가 설치된 다음에 쓸모 있게 된다. 이 선택들은 조종탁과 수감기들이 서로 다른 체계들에 위치하고 있을 때 그것들이 리용하는 암호열쇠를 관리할수 있도록 하기 위한것이다. RealSecure는 조종탁과 수감기들사이의 각종 통신을 위하여 공개비밀열쇠쌍을 리용한다. 일단 선택이 만들어 지면 Next를 찰칵한다.

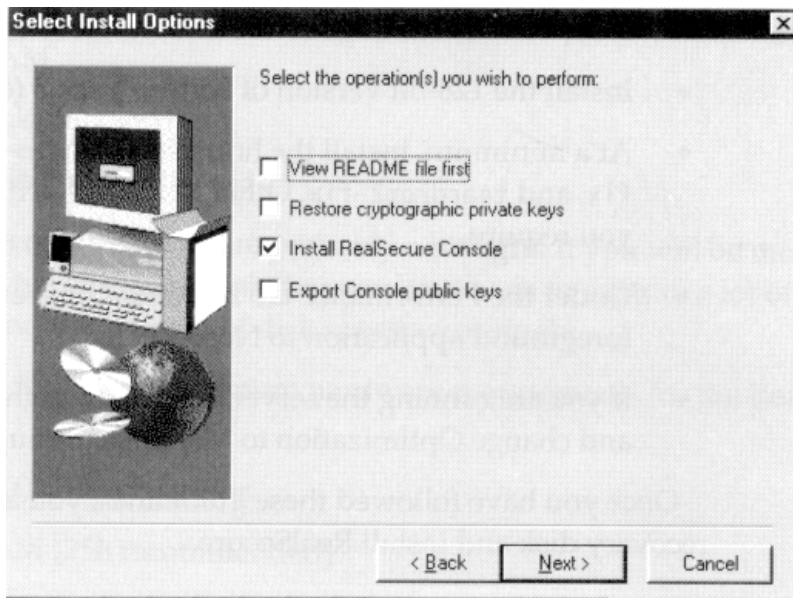
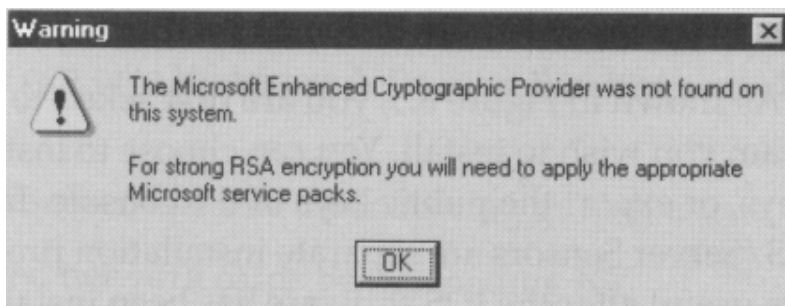



그림 8-5. Real Secure설치의 선택설치선정화면

그러면 RealSecure파일들의 목적지를 선택하라는 지령이 나오게 된다. 기정은 C구동기상에서 Program Files등록부아래 그것을 적재시키는것이다. 모든 RealSecure파일들이 자기의 고유한 위치에 적재되도록 이 경로를 D로 변경시킬것을 권고한다. 이것은 기록파일들이 구동기전체를 채우리만큼 아주 커진다 해도 체계기능에 영향을 주지 않도록 담보하는데 도움을 준다. 일단 새로운 경로가 확정되면 계속하여 Next를 찰칵한다.

일단 자기 파일에 대한 위치가 결정되면 높은급암호화판봉사묶음이 설치되지 않았다는것을 체계가 검출할 때 다음과 같은 통보를 내게 된다.

경고를 접수하면 그림 8-6에서 보여 준것과 같은 Select Cryptographic Setup 화면이 나타난다.

이 화면은 암호봉사제공자(CSP)를 선택할수 있게 한다. CSP는 조종탁과 수감기들사이의 모든 자료흐름을 암호화 및 복호화하는 요소이다. Microsoft Base Cryptographic Provider는 Service Pack 3의 부분으로서 후에 설치된다. 결국 체계가 보강되게 된다. 만일 체계상에 제3자의 CSP를 설치했다면 역시 이 창문에 나타나게 된다.

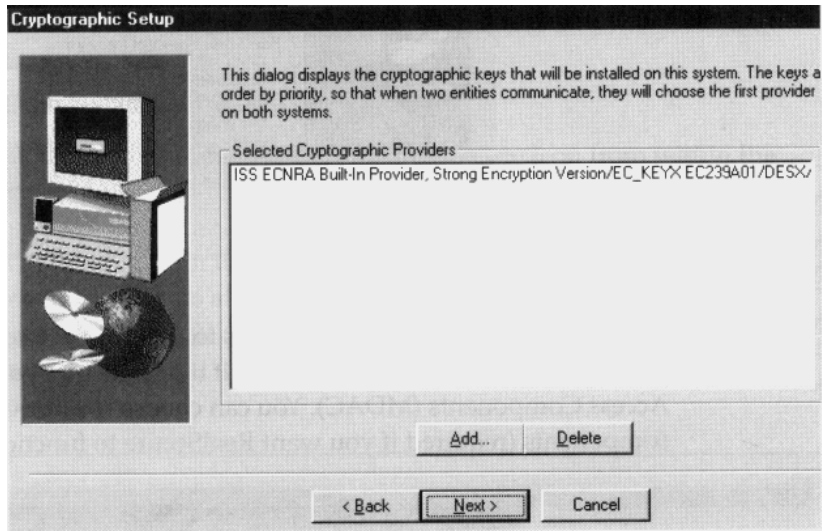



그림 8-6. 암호설치화면

강력한 암호를 리용하려고 한다면 Service Pack 6a의 128bit판을 리용하여야 한다. 어떤 Service Pace의 40bit판을 설치하였다면 약한 암호만을 리용할수 있다. 설치되여 있는 어떤 Service Pack의 40bit판만으로 강한 암호를 선택하게 되면 설치프로그람은 약한 암호가 리용될수 있다는것만을 경고한다. 약한 암호는 보통 방화벽뒤에서 리용하면 좋다. 그러나 공공망상에서 통신이 진행되고 있다면 강한 암호를 리용할것을 심중히 고려하여야 한다. 강한 인증을 위하여 약한 암호대신에 강한것을 사용하면 약간의 성능저하가 있게 된다. 그러나 안전은 더 강화된다.

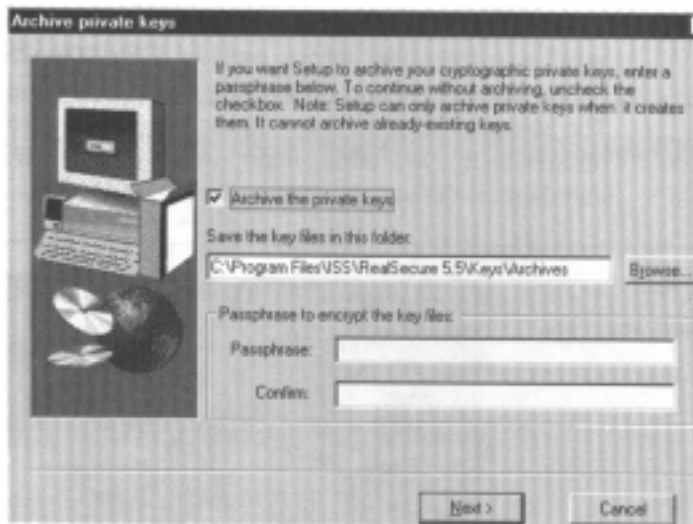
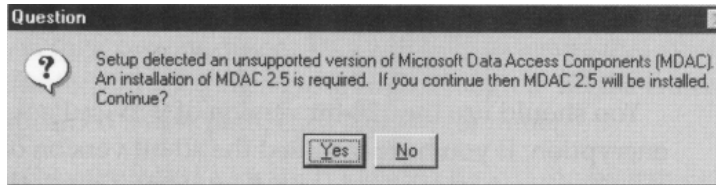
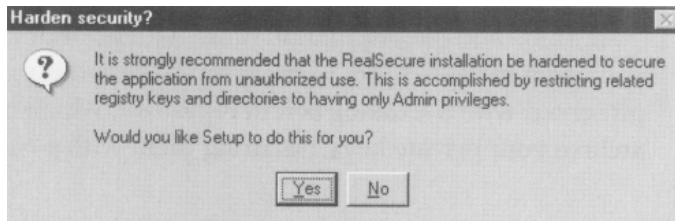



그림 8-7. RealSecure는 자기의 비밀열쇠를 보관할수 있다

이 점에서 설치프로그람은 프로그람묶음을 이름 짓고 체계에 파일들을 설치하기 시작한다. 일단 이 처리가 완성되면 그림 8-7에 있는 대화칸을 제공하는데 이것은 자기의 비밀열쇠를 보관할 기회를 제공하여 준다(통과성구를 가지고 그것을 보안한다.).

이 화면다음에 체계는 파일들을 복사하기 시작한다. 복사과정이 끝나가면 Microsoft의 자료접근성분(MDAC)들이 부족하다는것을 알고 체계는 지령통보를 내보낸다.

체계가 그 성분들(RealSecure가 적당히 기능할것을 원하는 경우에 요구된다.)을 설치하도록 선택할수 있다.

RealSecure가 최신MDAC를 설치한 다음(만일 요구된다면) 설치프로그람은 사용자에게 RealSecure가 사용하는 등록부들과 등록기열쇠에 대한 허용준위설정을 검사함으로써 보안을 강화하도록 지령을 준다. 이것은 체계관리자나 혹은 등가적인 구좌에 의하여서만 접근할수 있다는것을 담보하기 위한것이다.

주 의

NTFS를 리용하도록 구동기구역을 분할하였다면 NT봉사기에 대한 등록부허가만을 설정할수 있다.

이제는 설치가 완결되였다.

등록고의 변경이 유효로 되고 IDS수감기봉사가 시작되도록 하기 위하여 봉사기를 재기동하여야 한다. 수감기는 체계가 초기화되는 동안 자동적으로 시동된다. 그러나 조종탁은 RealSecure프로그람묶음으로부터 개시되여야 한다. 체계가 일단 재기동하면 RealSecure프로그람등록부에 ISS.KEY파일을 복사하여야 한다.

RealSecure구성

RealSecure조종탁을 시동하기 위하여 RealSecure프로그람묶음안에서 Real Secure그림기호를 선택한다. 그러면 그림 8-8에 보여 준 화면이 만들어 질것이다. 화면의 웃부분은 RealSecure 차림표이다.

그림 8-8. RealSecure조종탁화면

모든 기능은 내리펼침차림표나 혹은 도구띠를 통하여 작용한다. 화면아래에 수감기보기가 있다.

이 창문은 련속 감시를 받고 있는 모든 수감기들을 현시한다.

감시를 받지 않는 수감기는 자료를 여전히 수집하며 이 정보를 조종탁에로 쉽게 통지할수 없다.

감시할 조종탁을 선택하기 위하여서는 수감기차림표로부터 Sensor→Monitor Sensor를 찰칵하시오.

일러두기

모든 정보화면을 보기 위하여서는 800×600 혹은 그이상의 화면해상도를 리용해야 한다.

선택한 Monitor Sensor 는 Add Sensor 대화칸을 만들어 낸다. 감시하려는 모든 수감기들을 선택하기 위하여서는 이 창을 리용하여야 한다. 같은 콤퓨터상에 조종탁과 OS 또는 NetWork Sensor가 설치되여 있다면 국부호스트수감기에 대한 하나의 항목을 보아야 한다. 수감기가 원격콤퓨터상에 있다면 Add를 찰칵하고 IDS수감기의 IP주소에 기입해야 한다. 망상에 있는 매개 수감기에 대하여 이것을 수행한다. 다음에 원하는 매개 수감기를 눈에 띄우게 강조하고 그것들을 감시하기 위하여 OK를 찰칵한다.

수감기가 Sensor View우에 나타날 때 Maintenance 차림표를 만들기 위하여 특정의 수감기항목을 오른쪽찰칵할수 있다. 이 차림표로부터 주어 진 수감기의 특징들을 구성하기 위한 Properties를 선택하기 바란다.

그림 8-9. Network Sensor화면의 Policies표쪽

만일 Network Sensor를 선택하였다면 그림 8-9에 보여 준 Sensor Properties화면이 나타난다.

Network Sensor Properties 화면의 Policies창은 IDS가 리용할 보안방책의 형식을 정할수 있게 한다. 다음의 내용들을 선택할수 있다.

Web Watcher는 HTTP에 기초한 공격징후들을 모든 Web자료흐름에 적용한다.

PMZ Engine은 DMZ(비무장지대)안에서의 자료흐름을 분석하고 내부망으로 DMZ를 교차시키려는 시도들을 탐색한다.

Engine Inside FireWall은 내부망의 자료흐름을 주사하여 비정상적인것들을 찾는다.

For Windows Networks는 Windows자료가 아닌것을 화면에서 제거하는 방법으로 IDS체계를 최적화하면서 Windows에 기초한 징후들만을 망상의 자료에 적용한다.

Maximum Coverage는 모든 서명과 모든 통신규약모양을 허용하며 모든 결과를 조종탁에 보낸다.

Protocol Analyzer는 실제망자료를 보는데 리용된다. 징후들은 이 방책으로는 활성화되지 않는다. 그것들은 주로 망에 흐르는 자료들에 대한 어떤 생각을 관리자에게 주도록 하는데 리용된다.

Session Recorder는 NNTP, FTP, SMTP자료흐름을 위한 기정의 련결정보를 제공한다. 이 기정값들은 변경가능방책을 만들기 위하여 변형되게 된다.

Attack Detector는 아주 긴장한 자료만을 처리한다. 즉 이 방책은 망자료해신을 하지 않으며 정상적인 련결정보를 기록하지 않는다.

주　의

IDS수감기가 수행하여야 할 확인이 더 많을수록 요구되는 능력이 더 크다는것을 기억하여야 한다. 특정의 취약성들만을 검사하도록 여러가지 방책들이 설계되여 있다.

물론 방책은 정확히 맞지 않을수 있다. 그러므로 여기서는 방책들중의 하나를 견본으로 리용하여 요구에 부합되게 그것을 변경시키는 문제를 고찰한다. 임의의 기정방책들을 직접 편집할 대신에 가장 가까운것을 선택하고 Derive New Policy단추를 찰칵한다. 여기서 선택된 방책에 이름을 줄수 있다. 일단 이 과제가 수행되면 설치정형을 보기 위하여 Customize를 찰칵한다. 그러면 Policy Editor창문이 나타난다. Policy Editor는 보안과 련결사건들을 변경시키고 사용자정의된 사건들을 만들어 내며 려파기들을 설정하도록 하여 준다.

그림 8-10에서 보여 준바와 같이 창문 왼쪽에 개별표적들을 보여 주는 나무가 있고 오른쪽우에는 상세한 목록이 있다. 한편 오른쪽 아래에는 창문 왼쪽에서 선택된것에 대한 설명이 연시되여 있다.

그림 8-10. Policy Editor 화면의 Security Events표쪽

Security Events칸은 IDS가 어떤 공격을 감시하며 특정의 동작이 검출되였을 때 어떻게 작용할것인가를 설정할수 있게 한다. IDS수감기는 Enabled렬에서 검사된 매개 항목을 찾는다. 만일 어떤 특정의 작용에 대하여 안전하다는것을 안다면 그것에 대한 검사를 하지 않고 자원을 보호할수 있다.

실례로 어느 콤퓨터도 봉사로서 Finger를 돌리지 않는다면 Finger약점을 검사할 필요가 없다.

일러두기

특정의 약점에 대하여 항상 걱정을 하지 않아도 된다면 직결Help는 목록에 기입된 매개 약점에 대하여 훌륭한 설명을 준다. 약점에 대한 우려가 여전히 있다면 심중하게 대하는것이 좋으며 IDS가 취약성을 검사하게 하여야 한다.

Priority렬은 매 사건에 관하여 긴급성정도를 선택하게 한다.

그림 8-8로 되돌아 가보면 매개 우선권준위가 자기 창문에 현시되여 있는것을 보게 된다.

이것은 후에 조사하려는 자료흐름과 즉시적인 관심을 돌려야 할 자료흐름사이를 빨리 구별하도록 해준다.

또한 후에 보고할 항목들을 배렬하는데 도움을 주게 된다.

망에 대하여 설정한 우선권에 관계없이 Display칸은(Response렬아래) 세개의 조종탁 창문들중의 하나에 기입된 사건들을 발견하기 위하여 검사되여야 한다.

Response렬을 찰칵하면 그림 8-11에서 보여 준 Action대화칸이 나타난다.

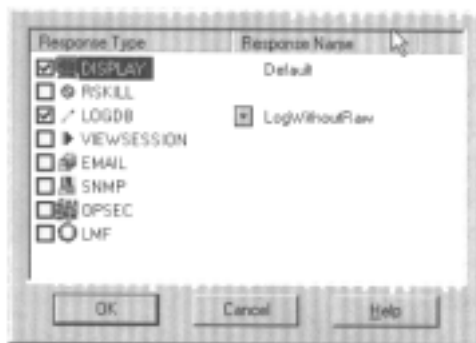



그림 8-11. Response대화칸

여기로부터 특정사건이 발견되였을 때 IDS수감기가 반응하도록 하는 방법을 선택할 수 있다. 이것은 사건을 단순히 기록하는 정도로 편리하거나 접속을 끊고 방화벽규칙을 변경시키며 전자우편이나 SNMP트랩통보를 통하여 사건통지문을 보내는것처럼 반응성이 좋을수 있다. 공격을 문서로 완전히 기록하기 위하여 파케트들의 원천자료를 기록할수도 있다.

Policy Editor차림표에서 Connection Events칸을 찰칵하면 그림 8-12에서 보여 준 화면이 제시된다. 더 작은 세분화를 요구할 때 Connection Events 화면을 리용하여야 한다. 실례로 DMZ망상에 있는 Web봉사기를 가지고 있다고 가정하자. Web봉사기가 외부세계로부터 련결을 기대한다고 하여도 이 체계는 다른 체계와의 그 어떤 련결도 설정할수 없다.

만일 그것이 발생한다면 Web봉사기는 다른 체계를 조사 혹은 공격하려고 하는 공격자에 의하여 손상될수 있다.

Connection Events설정을 리용하면 Web봉사기로부터 발생하는 모든 원천자료흐름을

감시하기 위한 3개의 방책규칙들을 쉽게 설치할수 있다. 세개가 요구되는것은 TCP를 위하여 한개 규칙, UDP를 위하여 한개 규칙, ICMP를 위하여 한개 규칙을 설치하여야 하기때문이다. 원천주소로는 Web봉사기의 IP주소를 리용하여야 한다. 이 체계에서 발생하는 모든 자료흐름을 통지하려고 하기때문에 목적지주소, 원천포구, 목적지포구를 Any로 설정한다.

주 의

이것을 강력한 도구로서 이상하다고 보는 사건외에도 더 많은것을 감시할수 있게 하여 준다. Connection Events 설정은 약점이 발견되지 않았다고 하여도 특정한 봉사를 감시하는데 리용될수 있다.

Edit Policy차림표의 User-Specified Filters칸은 IDS가 감시하지 않는 체계나 또는 특정의 봉사를 구성하도록 한다. 이것은 특정의 자료흐름이 기록되지 않도록 하려고 할 때 유용하다. 실례로 탁상체계IP주소에서 모든 HTTP자료흐름을 려과할수 있다(여기에는 이 특성에 대한 약간의 보안관련리유가 있을수 있다.).

마지막으로 Filters칸은 일부 규약, 접속형태, 자료흐름을 무시하게 한다. 특히 해커가 일반(DNS, FTP, HTTP 등)체계이상으로 봉사를 점유하고 있다고 의심하는 경우에 이것이 유익할수 있다. 포괄적인 방책을 확립하고 일반규약들을 무시하면 비정상적인 자료흐름모형들이 끝까지 남아 있을수 있다.

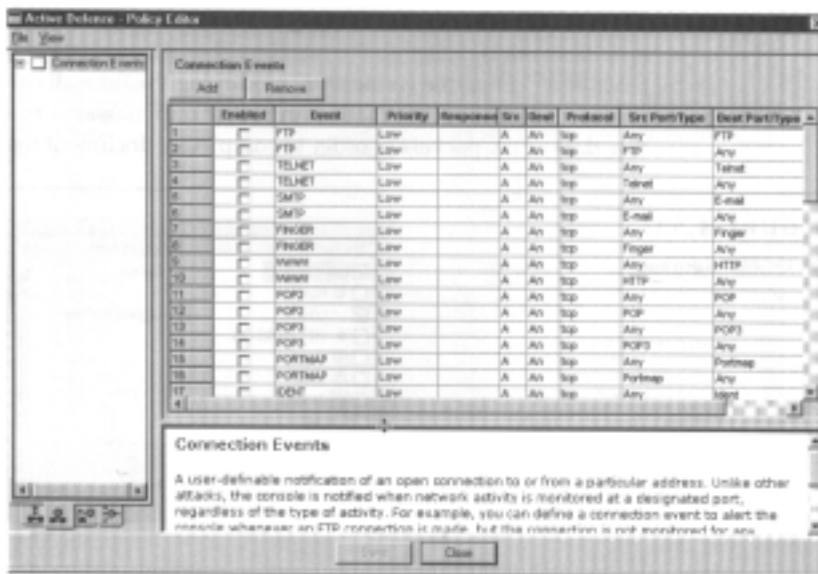



그림 8-12. Policy Editor차림표에서 Connection Events칸

수감기방책편집을 끝냈을 때 Sensor Properties화면에서 OK를 눌러 Policies칸에로 돌아 간다. 방책변화를 만들고 Apply to Sensor단추를 리용하여 그것을 적용한다. 이것은 수감기를 변경시키기 위하여 General칸조작을 앞으로 더 해나갈수 있게 한다.

General칸은 수감기구성에 대한 일반적인 정보를 보여 준다. 여기로부터 수감기가 실행하고 있는 쏘프트웨어판이 무엇이며 체계의 IP주소가 어떻게 되여 있는가를 알수 있다. 또한 조종탁과 송신하는 포구번호를 보거나 변화시킬수 있으며 수감기가 어떤 NIC를 감시하고 있으며 지어 RealSecure쏘프트웨어가 어느 등록부에 적재되여 있는가를 알수 있다. 보통은 이 설정을 변화시키지 않는다.

Alerts칸은 수감기가 오유, 경고, 정보알리기와 같은 NT Event Log를 쓸수 있다는것을 알리는 3개의 준위들을 결정한다. 매 준위는 허락 또는 금지로 될수 있다. 만일 허락되였다면 조종탁에 통지하거나 SNMP트랩을 제3자의 관리체계에로 보내도록 형성되게 할수 있다. Encryption칸은 모든 가능한 제공자들과 함께 현재의 암호제공자(수감기와 조종탁사이의 통신을 암호화하는데 리용되는 체계)를 보여 준다. 사용자가 OS수감기를 구성한다면 다음 칸에서 수감기를 위한 련결 및 검열설정을 정의한다. 마지막으로 Event Log칸은 NT Event기록으로부터 모든 수감기항목들을 밀어 내고 그것들을 창문에 연시한다. 이것은 혹시 수감기자체가 문제를 안고 있다면 수감기가 조작체계와 어떻게 호상작용하고 있는가를 관리자가 빨리 알수 있게 해준다.

응답들이 매개 개별적수감기방책에 대하여 구성될수 있다면 전체 응답들은 관리를 쉽게 하는데 리용될수 있다. View차림표에서 Global Responses의 항목들을 선택함으로써 그림 8-13에 보여 준 화면을 얻게 된다.

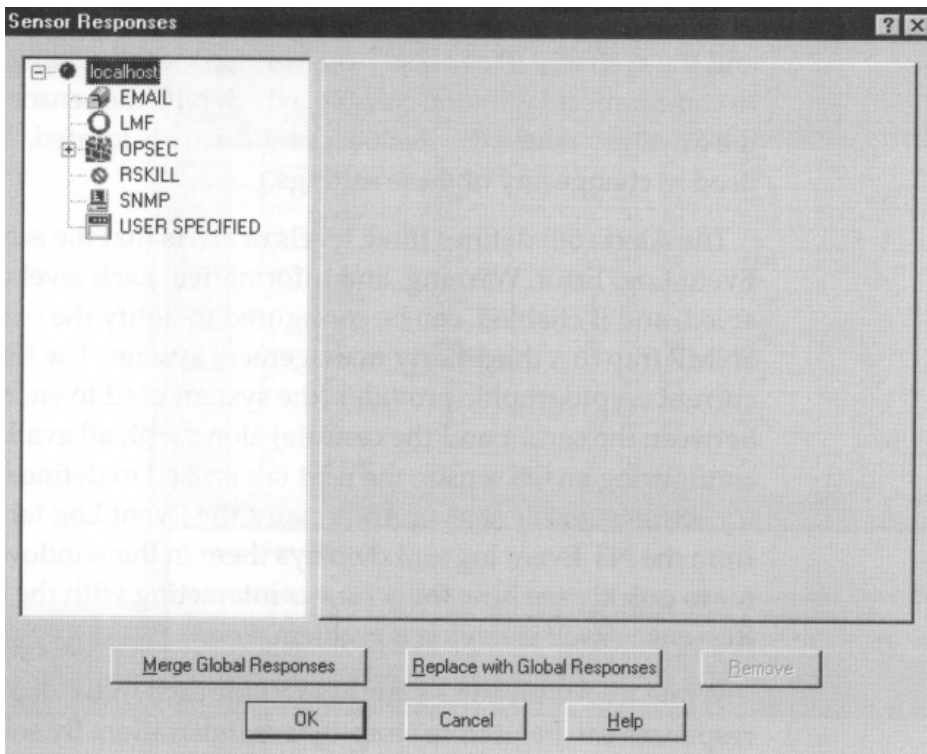



그림 8-13. 수감기속성화면의 Responses표쪽

변경가능한 이 화면우에는 일부 중요한 구성선택방안들이 있다. 가장 중요한것은 Tag RealSecure Kills 검사칸을 현시하는 RSKILL 항목이다. 이 칸이 검사되면 RealSecure는 대화중지를 위하여 리용된 모든 파케트들에 정보를 추가한다. 이것은 련결이 끊어 진 리유를 사람들이 알게 하여 준다. 자료흐름은 분석기 아니면 이러한 자료흐름을 보기 위하여 특별히 설계된 도구에 의하여 검사되여야 하지만 Realsecure가 련결을 중단하였다는것을 방송하는것은 수집하려는것보다 더 많은 정보를 손에 넣을수 있게 한다. IDS수감기를 보이지 않게 하려고 한다면 이 선택을 무효로 하여야 한다.

이 칸에는 련합작용항목을 리용하는데 요구되는 정보를 넣을수 있는 본문칸들이 있다. 실례로 만일 어떤 사건들에 대한 전자우편통보를 받으려고 한다면 우편통로와 예정 전자우편주소를 보장하여 주어야 한다.

다른 실례로서 Lucent와 Check Point 방화벽을 들수 있다. 창문의 왼쪽구역에 있는 LMF그림기호를 찰칵하면 그림 8-14에서 보여 준것과 같이 오른쪽구역에 Lucent Firewall 선택이 현시된다. 이 화면으로부터 사건들이 발생할 때 통지하여야 할 방화벽의 IP주소와 그것과 접촉하는데 리용할 열쇠를 지정할수 있다.

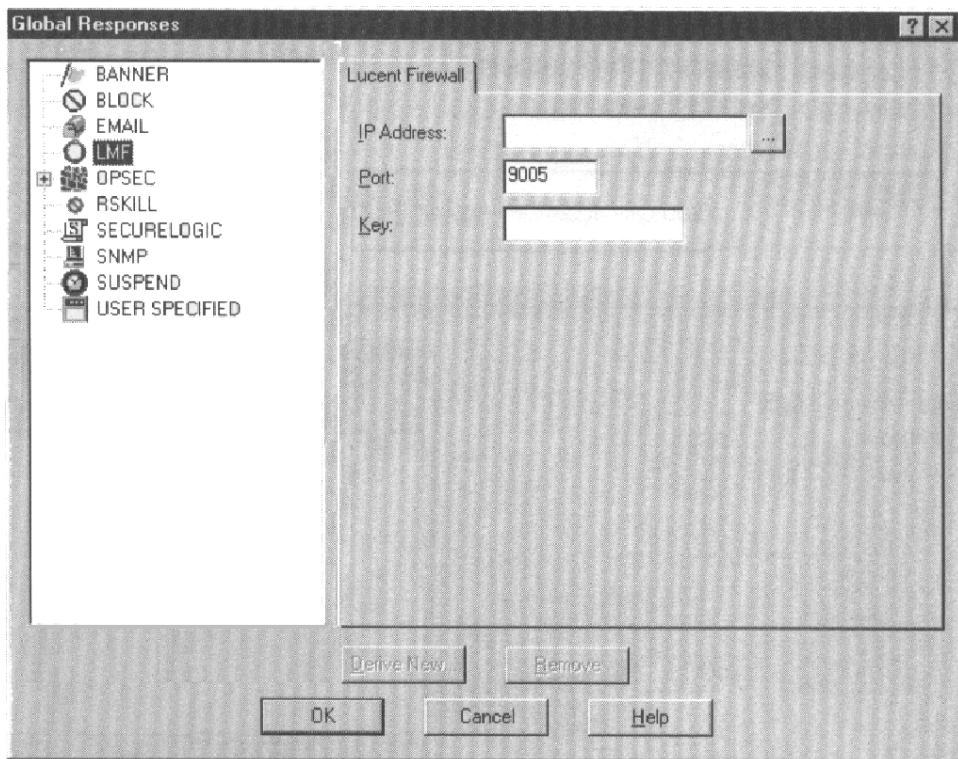



그림 8-14. Global Responses의 Lucent 방화벽의 화면

LMF아래에 있는 선택은 OPSEC이며 이것은 Check Point의 방화벽-1을 가리킨다. 이 창의 선택들은 Notify를 포함하며 방화벽-1이 기록된 사건들을 어떻게 기입하겠는가를 지정하게 한다.

Action항목은 방화벽이 사건에 어떻게 응답하며 단순히 통지만 할것인가, 사건을 금지시키는가 또는 금지시키고 련결을 끝내는가를 지정한다. Fire Wall Host는 어느 방화벽 경로기들이 영향을 받는가에 따라 통로장치들 혹은 관리자가 지적하는 다른 장치들을 확정한다.

Inhibit Expiration 선택은 규칙변경이 수행되겠는가 아니면 지정된 시간주기 이후에 제거되겠는가를 지정할수 있게 한다. 마지막으로 Initialization Settings와 Event Port 선택들은 IP주소와 방화벽-1관리봉사기의 도구번호를 지정한다.

일단 수감기구성변경을 끝내면 체계(변경이 Global Responses 페지로 만들어 지는 경우) 혹은 Responses 창문의 수감기에 그 변경을 적용한다. OK를 찰칵하고 체계 또는 수감기에 대한 변경을 하고 이러한 새로운 방책에 따라 앞으로의 모든 자료흐름감시를 수행한다.

주 의

여러개의 수감기인 경우에는 매개에 대한 구성단계대신에 Global Responses를 리용하여야 한다.

사건감시

RealSecure 조종탁에서 사건들을 감시할수 있다. 화면의 오른쪽에 있는 Priority 창문들은 일단 사건들이 발견되면 그것들을 현시하기 시작한다.

어느 한 보호체계에 대한 공격을 개시하는 방법으로 한개 사건을 발생시키려고 할수 있다. 공격시도가 없다면 간단한 포구주사로서 IDS수감기가 작업중이라는것을 충분히 확증할수 있다.

화면의 왼쪽은 RealSecure조종탁의 Active Tree인데(그림 8-15) 그것은 원천IP주소, 목적지IP주소 또는 특수사건에 따라 모든 최근의 작용을 빨리 분류할수 있게 해준다. 이것은 무슨 자료흐름이 망을 통과하였는가를 결정할수 있는 아주 유력한 도구이다. 실례로 그림 8-15의 긴급보기는 24.6.91.205 IP주소에서 그 누군가가 NetBIOS대화를 통하여 이 NT체계(IP주소24.92.184.100)에 접근하려고 시도했다는것을 보여 준다.

일러두기

매 검출된 취약성에 대하여 오른쪽찰칵함으로써 그것의 약점서술에 접근할수 있다.

그림 8-15. Activity Tree창문의 Events표쪽

좋은 IDS를 가지고 수집할수 있는 상세한 정보의 량은 매우 많다. 실례로 그림 8-16에 제시된것처럼 체계접근시도를 앞으로 연구하려고 한다고 하자. 이 사용자들이 무엇을 하고 있는가를 더 잘 보기 위하여 Source 칸을 찰칵한다.

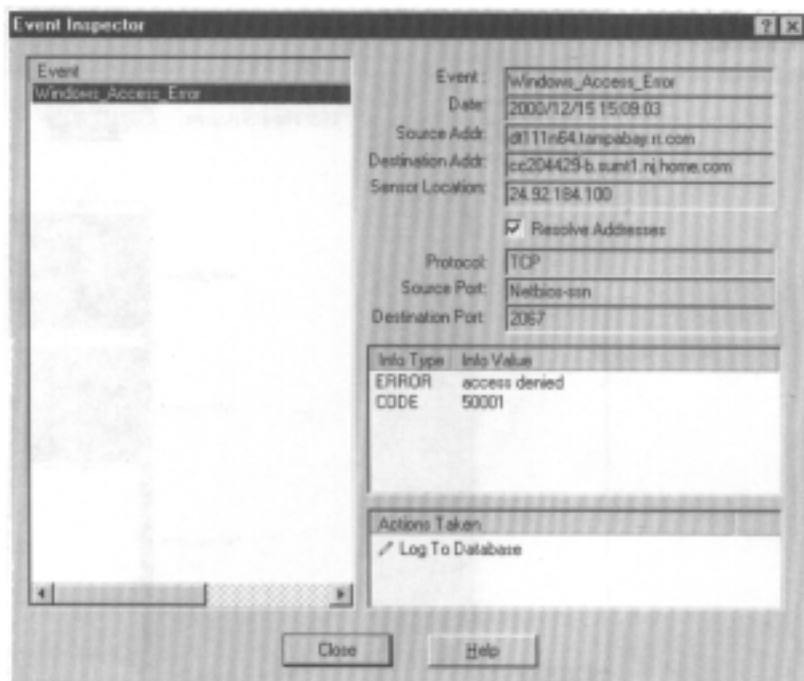



그림 8-16. 사건감시창문

어디서 매개 콤퓨터가 가동하고 있는가를 정확히 알수 있을 때까지 나무를 펼치면서 가지뻗기를 계속 할수 있다.

나무배비도의 제일 아래준위에서 개별적사건을 오른쪽찰칵함으로써 감시사건선택을 취할수 있다. 이것은 사건감시기창문을 만들며 상세도의 높은 준위 즉 작용이 가해 진데 따라서 원천과 목적지IP주소, 통신규약, 원천과 목적지포구(정보형태와 값을 포함한다.)를 제공하여 준다. 실제상 령역이름에 요청을 보내는 체계의 IP주소를 변환할수 있다(그림 8-16을 보시오.). 이것은 유익한데 령역이름을 알면 령역이름소유자와 접촉할수 있으며 결국 특정의 체계에 대한 작용을 추적할수 있다.

이것은 해커를 발견할수 있다는 담보로는 되지 않지만 적어도 체계에 침투할 목적으로 리용된 한개의 접근수단을 배제할수 있다. 그림 8-16에서 봉사기에로의 망련결요청이 home.com 령역상의 콤퓨터로부터 온다는것을 알수 있다(이것은 @Home, AT&T의 케블모뎀 ISP에 관하여 예약된 이름이다.). 령역이름소유자들로부터 접촉정보를 알기 위하여 WHOIS질문을 할수 있다. @Home은 개별콤퓨터이름이 붙은 사용자들의 통과흔적을 유지보존하며 그것들은 자기의 의뢰자들에 의한 체계의 무효조사를 금지하는 방책을 직접 리용한다.

Destination칸은 많은 항목들을 가지고 있다. 차이점은 나무가 목적지 IP주소 또는 호스트이름을 배렬한다는것이다. 가지들을 따라 가면서 매개 주소에 누가 접근했는가와 무슨 자료흐름이 발생했는가를 알수 있다.

보고기능

침입검출체계는 상세한 요약관리보고기능이 없이는 완성되였다고 볼수 없다. RealSecure조종탁으로부터 보고를 하도록 하기전에 매개 수감기자료기지에 기록된 자료를 보내야 한다. 이것을 RealSecure조종탁차림표에서 File → Synchronize All Log를 설정하는 방법으로 수행한다.

모든 자료가 조종탁에 전송된후에 보고기능을 기동할수 있다. Real Secure조종탁차림표에서 View→Reports를 선택한다. 체계는 미리 준비된 많은 보고 기능을 포함하고 있다. Top 20 Events보고화면이 그림 8-17에 제시되였다.

Top 20 Events보고는 망우에서 무엇이 일어 났는가를 20,000피트눈금으로 보여 줄수 있게 설계되였다. 더 상세한 내용이 요구된다면 왼쪽렬로 배렬되여 있는 어느 한 사건을 선택할수 있다. 그러면 그 사건의 매개의 기록된 실례들을 보여 주는 추가적인 본문보고를 보여 준다. 물론 모든 보고내용들은 RealSecure조종탁이 국부망 또는 망인쇄기에 접근을 가지고 있다면 인쇄될수도 있다.

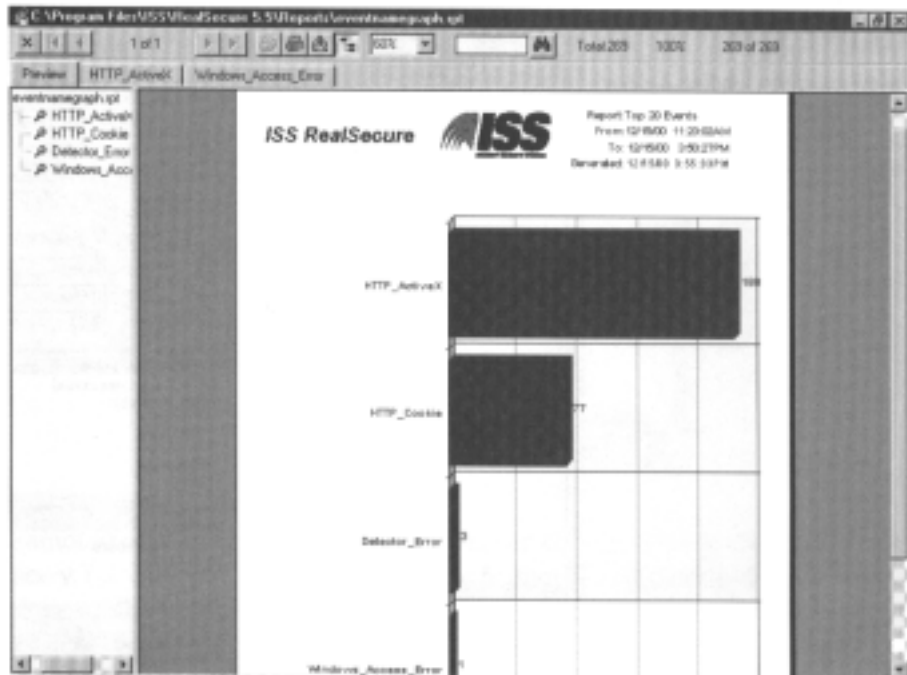



그림 8-17. Top 20 Events에 대한 보고

보고내용에 관심하는것이 없다면 요구에 맞는 새로운 보고내용을 지정할수 있다. 조종탁자료기지는 ODBC-호환성을 가지며 따라서 Microsoft Access와 같은 ODBC-호환의 자료기지프로그람을 가지고 자료파일을 읽을수 있다. 이것은 RealSecure 체계에 의하여 수집된 정보를 해석하고 보고하는데서 보다 더 좋은 유연성을 보장하여 준다.

요 약

이 장에서는 침입검출체계의 기초와 그것이 망환경을 보안하는데 어떻게 리용되는가를 보았다. IDS제품들의 일부 우결함을 일반적으로 알게 되였다. 잘 판매되고 있는 IDS 제품들중의 하나인 RealSecure의 설치와 구성에 대하여서도 취급하였다.

다음장에서는 인증과 암호화기술을 고찰하게 된다. 이것은 안전이 보장되지 않은 망통로에 련결되여 있는 기관들에서 매우 중요한 문제이다.

제9장. 인증과 암호화

인증과 암호화는 자료의 안전을 보장하기 위하여 호상 련관된 두가지 기술이다. 인증은 서로 통신하고 있는 쌍방이 실제로 자기들이 옳다는것을 담보하는 과정이다. 이것은 봉사에 가입하려는 실체(말단사용자)뿐아니라 봉사를 제공하는 실체(봉사기 또는 Web싸이트)에 대하여서도 마찬가지로 적용된다. 암호화는 대화조종과정에 정보가 손상되지 않는다는것을 담보한다. 《손상》이라는 의미는 자료흐름에서 정보의 읽기만이 아니라 그것의 변경도 포함하고 있다.

인증과 암호화는 각기 자체의 고유한 통신대화의 보안을 보장하여야 할 책임을 가지고 있지만 최상의 보호는 이 두가지가 결합될 때에만 이룩될수 있다. 이러한 리유로 하여 많은 보안통신규약들이 이 두가지 특성을 다 포함하고 있다.

보다 높은 보안을 위한 요구

현재 인터네트상에서 리용되는 IP판본 4가 1970년대에 개발되였을 때까지만 하여도 망보안은 기본관심사가 아니였다. 체계보안이 중요하였지만 정보교환에 리용되는 전송에는 주의가 적게 돌려 졌다. IP가 처음으로 개발되였을 때 그것은 자기의 고유한 보안표준을 가지지 못하였다. IP규약은 IP가 전송하고 있는 자료를 보호하여야 한다는것을 고려하지 않았다. 앞으로 IP판본 6으로 교체된다고 하여도 그것이 널리 퍼지기에는 여러해가 걸릴수 있다.

평문전송

IP는 일반적으로 평문자료들을 전송하는데 이것을 보통 순수한 상태의 전송이라고 한다. 이것은 자료가 주파수변경 또는 재배렬없이 단순히 원래의 형태로 전송된다는것을 의미한다. 전송되는 자료에는 자료와 함께 인증정보가 포함된다. 이 처리과정을 그림 9-1에서 설명한다.

그림 9-1. 인증대화를 시작하는 파케트의 해신

그림 9-1은 통신대화에 대한 망분석기보기창을 보여 준다. POP3우편의뢰기를 가지고 우편을 검색하려는 사용자가 있다고 하자. 파케트 3~5는 련결을 초기화하는데 리용된 TCP 3-파케트신호교환이다. 파케트 6, 7은 POP3우편봉사기에 의뢰기가 련결 및 준비되였다는것을 알려 준다. 파케트 8로부터 매우 흥미 있는 정보들을 알수 있다. 그림 9-1의 아래부분을 보면 파케트 8에서 자료마당의 복호화된 내용을 알수 있다. 지령 USER는 POP3봉사기에 POP3의뢰기의 가입등록이름을 보내는데 리용된다. USER지령다음의 본문은 체계인증을 시도하는 사용자의 이름이다.

그림 9-2는 이 가입등록이름에 대한 POP3봉사기의 응답을 보여 준다. 파케트 9의 내용으로부터 가입등록이름이 접수되였다는것을 알수 있다. 이 가입등록이름은 그림 9-1에서의 가입등록이름과 같다. 만일 사용자의 통과암호를 알수 있다면 체계에 접근하여 충분한 정보를 얻을수 있을것이다.

No.	Source	Destination	Layer	Summary	Error	Size	Interpacket Time	Absolute Time
6	0020AF247F25	0000E82F772A	tcp	Port:POP3 ---> 1067 ACK PUSH		97	49 ms	8:58:38 PM
7	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK		64	192 ms	8:58:38 PM
8	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK PUSH		71	326 ms	8:58:38 PM
9	0020AF247F25	0000E82F772A	tcp	Port:POP3 ---> 1067 ACK PUSH		77	7 ms	8:58:38 PM
10	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK		64	162 ms	8:58:39 PM
11	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK PUSH		74	326 ms	8:58:39 PM
12	0020AF247F25	0000E82F772A	tcp	Port:POP3 ---> 1067 ACK PUSH		91	920 µs	8:58:39 PM
13	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK		64	172 ms	8:58:39 PM

```
 0: 00 00 E8 2F 77 2A 00 20 AF 24 7F 25 08 00 45 00 |..../w*. .$.%..E.
10: 00 3B 1C 00 40 00 20 06 BA CC C0 A8 01 64 C0 A8 |.;..@. ......d..
20: 01 3C 00 6E 04 2B 00 0D ED 56 00 BF 06 DF 50 18 |.<.n.+...V....P.
30: 22 2B D3 D6 00 00 2B 4F 4B 20 75 73 65 72 20 61 |"+....+OK user a
40: 63 63 65 70 74 65 64 0D 0A                      |ccepted..
```

그림 9-2. 가입등록이름을 접수하는 POP3봉사기

그림 9-3에서 파케트 11의 복호화된 내용을 볼수 있다. 이것은 POP3우편의뢰기가 봉사기에 보내는 다음의 지령들이다. 지령 PASS는 의뢰기가 통과암호렬을 보내는데 리용된다. 이 지령다음의 본문은 체계인증을 시도하는 사용자의 통과암호이다. 여기서 알수 있는것처럼 통과암호는 평문으로 보인다.

No.	Source	Destination	Layer	Summary	Error	Size	Interpacket Time	Absolute Time
6	0020AF247F25	0000E82F772A	tcp	Port:POP3 ---> 1067 ACK PUSH		97	49 ms	8:58:38 PM
7	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK		64	192 ms	8:58:38 PM
8	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK PUSH		71	326 ms	8:58:38 PM
9	0020AF247F25	0000E82F772A	tcp	Port:POP3 ---> 1067 ACK PUSH		77	7 ms	8:58:38 PM
10	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK		64	162 ms	8:58:39 PM
11	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK PUSH		74	326 ms	8:58:39 PM
12	0020AF247F25	0000E82F772A	tcp	Port:POP3 ---> 1067 ACK PUSH		91	920 µs	8:58:39 PM
13	0000E82F772A	0020AF247F25	tcp	Port:1067 ---> POP3 ACK		64	172 ms	8:58:39 PM

```
 0: 00 20 AF 24 7F 25 00 00 E8 2F 77 2A 08 00 45 00 |...$.%.../w*..E.
10: 00 38 89 05 40 00 80 06 ED C9 C0 A8 01 3C C0 A8 |.8..@........<..
20: 01 64 04 2B 00 6E 00 BF 06 DF 00 0D 0D 69 50 18 |.d.+.n.......iP.
30: 21 FE B8 5E 00 00 50 41 53 53 20 6D 69 63 72 6F |!..^..PASS micro
40: 24 6F 66 74 0D 0A                               |$oft..
```

그림 9-3. 사용자의 통과암호를 보내는 POP3의뢰기

그림 9-4에서는 파케트 12의 해신된 내용을 볼수 있다. 이것은 인증시도에 대한 봉사기의 응답이다. 봉사기가 가입등록이름과 통과암호결합을 접수한다는것에 주목하여야 한다. 우의 과정은 정당한 가입등록이름과 통과암호를 가지고 체계의 접근을 얻기 위한

인증처리과정이다. 사실 파케트들을 해신할수 있는 사람이라면 이 사용자의 모든 전자우편통보문들을 볼수 있다.

그림 9-4. 인증시도를 접속하는 POP3봉사기

평문피동감시

이 POP3인증대화는 망분석기를 리용하여 얻는다. 망분석기는 전용하드웨어도구나 현존 체계우에서 실행되는 쏘프트웨어이다. Windows 혹은 Mac플래트홈용망분석기쏘프트웨어는 천딸라미만으로 구입할수 있으며 UNIX에서 자유롭게 리용할수 있다.

망분석기들은 실제적으로 자료흐름을 감시하기 위하여 망우의 모든 자료를 다 전송할 필요가 없다는 의미에서 피동장치들이다. 어떤 분석기들은(보통 관리상태를 알아 내기 위한 목적에서)자료흐름을 전송하는데 이것은 꼭 필요한것은 아니다. 사실상 분석기는 유효한 망주소를 요구하지도 않는다. 이것은 망분석기가 망을 감시할수 있다는것을 의미하며 케블추적과 집선기 및 교환기포구들을 조사하지 않고서는 그것의 존재를 알아낼수 없다는것을 의미한다.

공격자는 손상된 체계우에 망분석기쏘프트웨어를 설치할수 있다. 이것은 공격자가 자료흐름을 감시하기 위하여 설비에 물리적으로 접근할 필요가 없다는것을 의미한다. 공격자는 간단히 현존 체계들중의 하나를 리용하여 목적하는 자료흐름을 얻을수 있다. 그러므로 체계들에 대한 정상적인 검열을 진행하는것이 아주 중요하다. 누구도 피동감시공격을 알아 차리지 못하는것을 원치 않을것이다.

망분석기가 통신대화를 얻기 위하여서는 대화경로의 어느 한 곳에 련결되여야 한다. 이것은 망우에서 대화를 시작하는 체계와 목적지체계사이의 어느 한점이 될수 있다. 이것은 또한 대화의 어느 한쪽끝에 있는 체계를 손상시킴으로써 실현할수도 있다. 이것은 공격자가 원격위치에서 인터네트상의 망자료흐름을 얻을수 없다는것을 의미한다. 공격자는 반드시 망내부에 어떤 형태의 감시기나 분석기를 배치하여야 한다.

주 의

4장에서 설명한바와 같이 망다리, 교환기, 경로기들을 리용하면 분석기가 얻으려는 자료량을 줄일수 있다.

평문통신규약

POP3은 평문으로 통신하는 유일한 IP봉사는 아니다. 거의 모든 IP봉사들이 인증과 암호화를 제공하지 않으며 평문으로 자료를 전송한다. 일부 평문봉사들은 다음과 같다.

FTP 인증은 평문이다.
Telnet 인증은 평문이다.
SMTP 우편통보문의 내용은 평문이다.
HTTP 홈안에 있는 페지내용과 마당내용들은 평문이다.
IMAP 인증은 평문이다.
SNMPv1 인증은 평문이다.

경 고

SNMPv1이 평문을 리용한다는것은 특히 좋지 않다. SNMP는 망장치들을 관리하고 문의하는데 리용된다. 이러한 장치들에는 교환기와 경로기 지어 봉사기와 방화벽까지도 포함된다. SMTP통과암호가 손상되면 공격자는 망에 커다란 피해를 줄수 있다. SNMPv2와 SNMPv3은 열린최단경로규약(OSPF)과 류사한 통보문알고리듬을 포함한다. 이것은 원래의 SNMP보다 높은 준위의 안전성과 자료완전성을 보장한다. 유감스럽게도 많은 망장치들이 SNMPv3은 물론 SNMPv2도 지원하지 못하고 있다. 현재는 SNMPv1이 널리 리용된다.

인증의 필요성

좋은 인증에 대한 요구는 지금에 와서는 명백한것으로 되였다. 평문으로 전송되는 가입등록정보는 감시하기 매우 쉽다. 쉽게 해득될수 있는 가입방법은 통과암호가 변경되지 않는 환경에서 보다 큰 문제를 발생시킬수 있다. 이러한 경우 공격자는 손상된 구좌를 리용하여 망을 쉽게 공격할수 있다. 많은 사용자들은 모든 구좌에 대하여 같은 가입등록이름과 통과암호를 오래동안 리용하려고 한다. 이것은 POP3과 같은 안전이 담보되지 않은 봉사로부터 인증증서를 얻을수 있는 경우 NT나 NetWare봉사기들과 같은 망의 다른 체계들에 대한 정당한 가입등록이름과 통과암호를 가질수 있다는것을 의미한다.

좋은 인증은 가입초기에 봉사접속을 하려는 원천들이 정당한가를 확인한다. 또한 통신대화과정에 원천이 공격하는 호스트에 의하여 교체되지 않았는가를 확인하여야 한다. 이러한 형태의 공격을 흔히 대화가로채기라고 한다.

대화가로채기

그림 9-5에 보여 준 망을 고찰하자. 의뢰기는 봉사기와 불안전한 망련결상태에서 통신하고 있다. 의뢰기는 이미 봉사기에 인증되였고 접근이 허락되였다. 한가지 흥미 있는 실례를 만들어 보자. 의뢰기가 관리자준위특권을 가진다고 가정하자. 공격자는 의뢰기와 봉사기사이의 망토막에 있고 대화를 감시하면서 대화에 리용되는 포구와 순서번호들을 알아 낸다.

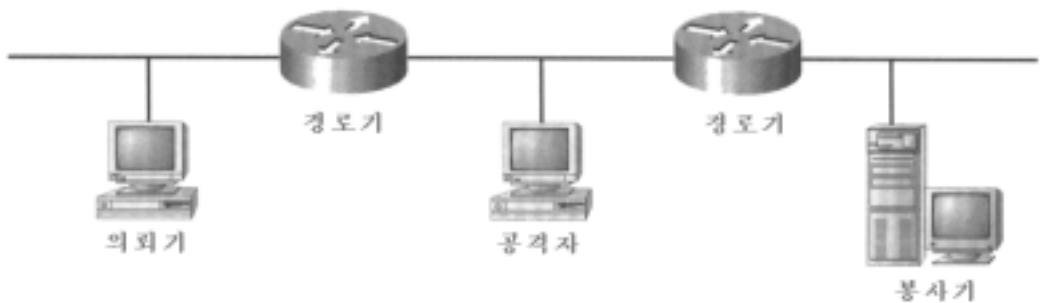



그림 9-5. 중개자공격의 실례

이제 공격자가 관리자준위의 특권을 가진 새로운 구좌를 만들기 위하여 관리자의 대화를 가로채려 한다고 가정하자. 먼저 공격자는 의뢰기가 봉사기와 더는 통신할수 없는 상태로 만들어 놓는다. 이를 위하여 공격자는 WinNuke와 같은 도구프로그람을 리용하든가 또는 죽음의 Ping을 보내여 의뢰기를 정지시킨다. 또한 ICMP범람과 같은 공격으로 정지시킬수도 있다. 어떤 형태의 공격을 진행하든 그 목적은 의뢰기가 봉사기에서 보낸 자료흐름에 응답할수 없도록 하는것이다.

주 의

ICMP범람의 목표로 된 체계는 ICMP요구에 응답하는데 많은 시간을 소비하기때문에 다른 통신들은 진행할수 없다.

결국 의뢰기가 마비되고 공격자는 마치 자기가 의뢰기인것처럼 봉사기와 자유롭게 통신하게 된다. 공격자는 의뢰기에로 오는 봉사기의 응답을 받아 적당한 응답을 만든다. 만일 공격자가 IP에 대한 상세한 지식을 가지고 있다면 봉사기로부터 예견되는 응답에 기초하여 봉사기의 응답과 전송포구 그리고 순서번호들을 완전히 무시해 버릴수 있다. 어느 경우에나 공격자는 봉사기가 여전히 원래의 의뢰기와 통신하고 있는듯이 만들어 놓는다.

결국 좋은 인증에서는 원천체계가 다른 체계와 바꾸어 지지 않았다는것을 확증하여야 한다. 이것은 두 체계가 통신대화과정에 서로 비밀정보를 교환하는 방법으로 해결할수 있다. 비밀정보는 대화과정에 전송되는 매 파케트마다 또는 우연시간간격으로 교환할수 있다. 명백히 매 파케트마다 원천을 확인하는것이 우연시간간격으로 원천을 확인하는것보다 훨씬 더 안전하다. 통신대화과정에 매 파케트를 교환할 때마다 비밀정보를 바꾸면 보다 안전하다. 이렇게 하면 대화는 대화가로채기에 보다 안전하도록 할수 있다.

목적지확인

통신대화가 시작된 때로부터 전 과정에 원천을 확인하여야 한다는것은 명백하다. 그러나 봉사기를 확인할데 대한 요구는 명백하지 않다. 많은 사람들은 자기의 봉사기에 련

결하거나 어떤 형태의 호스트로부터 도달불가능한 통보문을 받는것을 당연한것으로 생각하고 있다. 그러나 그들이 대화하고 있는 봉사기가 사실상 망을 공격하려는 공격자일수도 있다는것은 모를수 있다.

C2MYAZZ

도구프로그람 C2MYAZZ는 대화가로채기 혹은 중개자로 알려 진 봉사기속임공격의 전형적인 실례이다. Windows 95가 처음으로 나왔을 때 그것은 대화통보문블로크(SMB)체계에 인증하는 두가지 방법을 가지고 있었다. 암호화된 통과암호를 리용하여 인증하는것이 기정으로 되여 있었다. Windows NT령역에서의 인증에도 이 방법이 리용되였다. 그러나 SMB LANMAN봉사기와의 아래방향호환성을 보장하기 위하여 LANMAN인증도 리용되였다. LANMAN은 가입등록이름과 통과암호를 평문으로 전송할것을 요구한다. C2MYAZZ이 기동하면 그것은 의뢰기가 NT봉사기에 인증될 때를 피동적으로 기다린다. 가입등록이 검출되면 C2MYAZZ는 LANMAN인증을 요구하는 하나의 파케트를 의뢰기에 보낸다.

의뢰기는 이 파케트를 가입등록을 요구한 봉사기에서 보낸것으로 믿고 증서를 평문으로 다시 전송한다. 이때 C2MYAZZ도구프로그람은 가입등록이름과 통과암호를 획득하여 현시한다. C2MYAZZ는 의뢰기의 대화를 파괴하지 않고 사용자가 여전히 가입하여 체계접근을 실현할수 있게 한다. 이 도구프로그람의 특징은 하나의 기동디스크로 실행할수 있다는것이다. 다시 말하여 공격자는 이 디스크로 체계를 기동시킨 후에 얻어 진 증서를 가지기만 하면 된다.

주 의

> Microsoft는 이 취약성에 대한 수정보충프로그람을 발표하였다. 이 프로그람은 모든 Windows 95워크스테이션에 설치하여야 한다. Windows의 그이상의 판본들에서는 이 취약성을 극복하였다.

DNS중독

인증을 필요로 하는 또 다른것은 DNS중독(poisoning)이다. 일명 캐쉬중독이라고도 하는 DNS중독은 실지 목적지로부터의 자료흐름을 변경시킬 목적으로 특정호스트에 대한 틀린 IP주소정보를 넘겨 주는 과정이다. Eugene Kashpureff는 1997년 여름에 이것이 가능하다는것을 증명하였다. 그는 DNS봉사의 취약성을 리용하여 InterNIC호스트들에 대한 요청을 AlterNIC라고 하는 자기의 대리령역이름등록싸이트로 돌렸다.

이름봉사기는 DNS문의에 대한 응답을 수신할 때 특별히 요구되지 않는 정보들은 무시하거나 응답의 원천을 확인하지 않는다. Kashpureff는 이 약점을 리용하여 정당한 응답에 가짜DNS정보를 포함시켰다. 응답을 수신한 이름봉사기는 유효정보뿐아니라 가짜정보도 보관한다. 결과 사용자가 InterNIC의 령역(례하면 whois질문에 리용되는 rs.internic.net)내에 있는 한 호스트의 주소를 알려고 하였지만 그는 AlterNIC의 령역내의 IP주소를 받게 되며 AlterNIC망우의 체계로 유도된다.

Kashpureff의 공격을 좀 더 고찰하면 몇가지 훨씬 더 심각한 문제점들을 얻어 낼수 있을것이다. 직결은행거래가 리용되던 때에 누군가가 은행의 Web싸이트로부터 자료흐름

을 돌려 놓았다고 생각해 보자. 은행자료흐름을 다른 봉사기로 돌려 놓기 위하여 캐쉬중독을 리용하는 공격자는 은행의 진짜봉사기와 꼭 같은것으로 보이도록 가짜봉사기를 만들수 있다.

은행의뢰기가 자기의 은행구좌들을 관리하기 위하여 은행의 Web봉사기에 인증하려고 할 때 공격자는 인증정보를 얻어 내고 간단히 체계가 현재 비직결상태라는것을 나타내는 기발창문을 사용자에게 보일수 있다. 의뢰기가 우연히 IP주소에서의 불일치를 알아차리지 못하는 이상 수자식증명서가 리용되지 않고서는 자기가 다른 싸이트로 돌려 졌다는것을 알수 없다.

주 의

수자식증명서는 이 장의 뒤에서 나오는 《수자식증명서봉사기》에서 서술한다.

자기가 인증하려고 하는 봉사기를 확인하는것은 의뢰기의 증서 또는 대화의 무결성을 확인하는것만큼 중요하다. 통신과정에 있는 이 세 문제점들은 모두 공격에 대하여 약하다.

암호화101

암호학은 정보를 후에 다시 회복할수 있는 다른 형태로 전송하는데 리용되는 기술들의 집합이다. 이 다른 형태를 암호문이라고 하며 그것은 암호화알고리듬과 암호열쇠에 의하여 만들어 진다. 암호알고리듬은 단순히 암호화하려는 정보에 적용되는 수학공식이다. 암호열쇠는 매번 정보를 알고리듬이 처리할 때 같은 계산조작을 리용하여 암호문이 유도되지 않도록 하기 위하여 알고리듬에 넣어 주는 보충적인 변수이다.

이제 수 42가 당신에게 있어서 극히 중요한 수이며 그것을 다른 사람들이 알지 못하도록 지키려 한다고 하자. 이 자료를 암호화하기 위하여 다음과 같은 암호알고리듬을 리용할수 있다.

자료 / 암호화열쇠 ＋ (2×암호화열쇠)

이 과정은 암호알고리듬 그자체와 암호열쇠 이 두가지에 달려 있다. 이 둘은 다 암호문을 만드는데 리용되며 암호문은 새로운 수값으로 된다. 암호문을 되살려 42를 얻어내려면 알고리듬과 열쇠를 다 가지고 있어야 한다. 열쇠를 리용하지 않는 씨저암호(Caesar ciphers)로 알려 진 덜 안전한 암호알고리듬도 있으나 이것은 암호열쇠의 보충적인 안정성을 가지지 못하는것으로 하여 그리 쓰이지 않는다. 암호문을 복호화하기 위하여 씨저암호알고리듬만 알면 된다.

주 의

쥴리우스 씨저는 암호화를 리용한 첫 사람들중의 하나로 인정되고 있다. 그는 자기의 군대에 통보를 보내기 위하여 간단한 형식의 암호화를 리용하였다.

암호화는 수학공식들을 리용하므로 다음의 내용들사이에는 공생관계가 이루어 진다.

- 알고리듬
- 열쇠
- 원래의 자료
- 암호문

이것은 이것들중 어느 세가지만 알면 4개를 다 유도해 낼수 있음을 의미한다. 례외로 되는것은 원래자료와 암호문의 결합을 알 때이다. 만일 이 두가지의 많은 실례들을 가지고 있다면 알고리듬과 열쇠를 복구해 낼수도 있다.

암호화방법

암호문을 만드는데는 두가지 방법이 있다.

- 흐름암호
- 블로크암호

두 방법들은 매 과정에서의 암호화자료량을 내놓고는 류사하다. 현대적인 암호화체계들은 블로크암호를 리용한다.

흐름암호

흐름암호는 자료암호화의 가장 간단한 방법들중의 하나이다. 흐름암호가 사용될 때 자료의 매 비트는 열쇠의 한 비트를 리용하여 련속적으로 암호화된다. 흐름암호의 고전적인 실례는 Vernam암호이다. 이것은 전신타자통신을 암호화하기 위하여 리용되였다. Vernam암호의 암호열쇠는 페지의 순환에 들어 있다. 전신전문이 기계에 들어 가면 자료의 한 비트가 열쇠의 한 비트와 결합하여 암호문을 만든다. 암호문의 수신자는 같은 페지의 순환을 리용하여 거꿀과정을 거쳐 본래의 전문을 되살려 낸다.

고정된 길이의 열쇠를 리용하는 Vernam암호는 여러개의 전문들로부터 얻어 진 암호문들을 비교하면 쉽게 정확히 추적해 낼수 있다. 흐름암호를 해득하기 더 어렵게 하려면 가변길이의 암호열쇠를 쓰면 된다. 이렇게 함으로써 암호문으로부터 식별해 낼수 있는 모형들을 막아 치울수 있다. 사실 자료 한 비트에 리용되는 암호열쇠를 우연적으로 바꾸어 수학적으로 해득하기 불가능한 암호문을 얻을수 있다. 왜냐하면 리용된 서로 다른 우연열쇠들이 암호열쇠를 깨려 하는 크래커에게 단서를 줄수 있는 어떠한 반복모형도 생성하지 않기때문이다. 암호화열쇠를 련속적으로 변화시키는 과정을 일회용보충(one-time pad)이라고 한다.

블로크암호

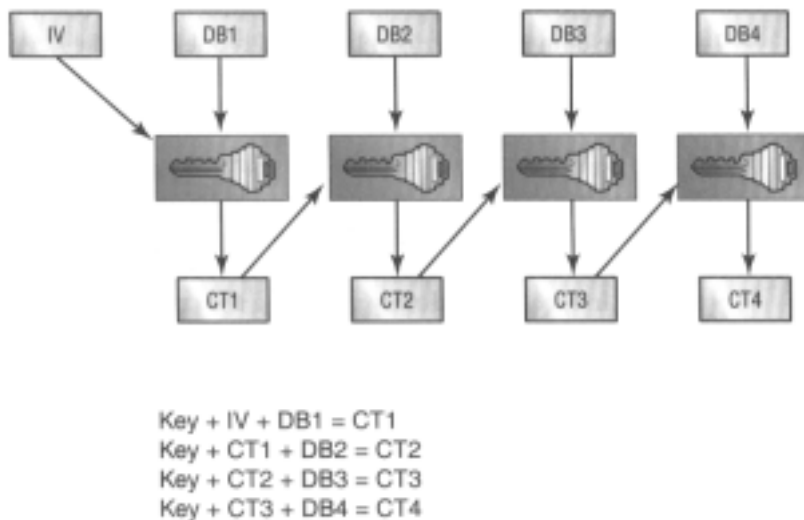
매 1bit를 암호화하는 흐름암호와는 달리 블로크암호는 일정한 크기의 덩어리단위로

자료를 암호화한다. 블로크암호에서 기본은 매번 얼마만한 자료가 암호화되며 어떤 크기의 열쇠가 매 블로크에 작용되는가 하는것을 확인하는것이다. 실례로 자료암호화표준(DES)은 암호화된 DES자료가 56bit의 열쇠를 리용하여 64bit블로크단위로 처리된다는것으로 정해 졌다.

블로크암호화를 실현하는데 리용하는 여러가지 서로 다른 알고리듬들이 있다. 가장 초보적인것은 간단히 자료를 택하여 그것을 블로크로 나누어 매개에 대하여 열쇠를 작용시키는것이다. 이 방법은 효과성은 높지만 반복되는 암호문을 만들수 있다. 만일 자료의 두 블로크가 정확히 같은 정보를 가지고 있다면 암호문의 두 블로크는 역시 동등할것이다. 앞에서 언급된것처럼 크래커는 비우연형식으로 반복된 암호문을 리용하여 암호열쇠를 공격할수 있다.

보다 좋기는 알고리듬의 보다 앞선 결과를 리용하여 보다 후의 열쇠들을 그것과 결합하는것이다. 그림 9-6에 변경시킬수 있는 한가지 방법을 보여 주었다. 암호화하려는 자료는 DB1～DB4로 이름 붙여 진 블로크들에 갈라 진다. 초기화벡토르(IV)가 자료의 시작에 첨부되여 모든 블로크들이 완전히 암호화되였다는것을 보여 준다. IV는 단순한 우연기호렬로서 두개의 동일한 통보문으로부터 같은 암호문을 만들어 내지 못한다는것을 담보한다. 암호문의 첫 블로크 (CT1)을 얻기 위하여 암호열쇠와 자료의 첫 블로크(DB1), 초기화벡토르(IV)를 수학적으로 결합한다.

Key + IV + DB1 = CT1
Key + CT1 + DB2 = CT2
Key + CT2 + DB3 = CT3
Key + CT3 + DB4 = CT4

그림 9-6. 블로크암호화

암호문의 두번째 블로크 CT2을 만들 때에는 암호열쇠암호문의 첫 블로크 CT1, 두번째 자료블로크 DB2을 수학적으로 결합한다. 알고리듬에서 변수들이 변하므로 DB1과 DB2은 같을수 있어도 결과적인 암호문 CT1과 CT2은 서로 다른 값을 가진다. 이것은 얻어 지는 암호문이 완전히 우연적인것으로 보이도록 충분히 혼잡될수 있게 한다. 얻어 지는 암호문을 리용하여 다른 자료블로크를 암호화하는 과정은 모든 자료블로크들이 처리될 때까지 계속된다.

암호열쇠와 초기화벡토르, 앞서 얻어 진 암호문을 수학적으로 결합하는 방법에는 여러가지가 있다. 이 모든 방법들은 다 같은 목적을 추구하고 있는데 그것은 보기에 우연적인 암호문의 문자렬을 얻어 내는것이다.

공개 및 비공개암호열쇠

지금까지 모든 암호화기술들은 비공개열쇠알고리듬들을 리용하였다. 비공개열쇠알고리듬은 암호화와 복호화에 같은 열쇠를 리용한다. 이것은 암호열쇠가 암호문의 안정성을 담보하기 위하여 비밀로 고수되여야 한다는것을 말해 준다. 만일 공격자가 그 비공개열쇠를 알아 낸다면 모든 암호화된 전문들을 풀어 낼수 있을것이다. 정보교환의 안전한 방법을 구축하기 위하여 비공개열쇠교환의 안전한 방법이 필요하게 된다.

1976년에 디피(W.Diffie)와 헬만(M.Hellman)은 론문 《암호학에서 새로운 방향》에서 공개열쇠암호의 개념을 제기하였다. 이 론문은 암호산업에서 혁명으로 되였을뿐아니라 공개열쇠의 생성과정은 지금도 Diffie-Hellman으로 알려 져 있다. 비전문가에 있어서 공개열쇠는 비공개열쇠로부터 수학적으로 유도된 암호열쇠이다. 공개열쇠로 암호화된 정보는 비공개열쇠로만 복호화할수 있으며 비공개열쇠로 암호화된 정보는 공개열쇠로 복호화할수 없다. 다른 말로 말하여 열쇠들은 대칭이 아니다. 그것들은 특수하게 구성되여 공개열쇠는 자료암호화에, 비공개열쇠는 암호문복호화에 리용되게 되여 있다.

이것은 열쇠정보를 교환하기 위한 안전한 통로가 요구되지 않게 한다. 공개열쇠는 암호화된 전문의 안전성을 여전히 유지하면서 불안전한 통로에서 교환할수 있다. 만일 한 사람이 친구에게 비밀전문을 보내려 한다면 그는 친구의 공개열쇠로 그것을 암호화해야 한다.

Diffie-Hellman은 인증을 제공하는데 리용할수도 있다. 이것은 수신자의 공개열쇠로 전문을 암호화하기전에 자기의 비공개열쇠로 그것에 서명하여 실현할수 있다. 서명은 자기의 비공개열쇠와 전문내용을 처리하는 간단한 수학적알고리듬이다. 이것은 유일한 전자서명을 만들어 내는데 그것은 전문의 뒤에 붙는다. 전문내용이 서명을 만드는데 리용되므로 전자서명은 보내는 매 전문에서 다를것이다.

실례로 어떤 사람이 친구에게 비밀전문을 보낸다고 하자. 먼저 그는 자기의 비공개열쇠를 가지고 전자서명을 하고 친구의 공개열쇠로 전문을 암호화한다. 친구가 전문을 받으면 먼저 자기 비공개열쇠로 암호문을 풀고 그의 공개열쇠로 전자서명을 검사한다. 서명이 맞으면 그는 전문이 인증된것이라는것과 그것이 전송과정에 바뀌지 않았다는것을 알게 된다. 만일 서명이 맞지 않으면 그는 전문이 그의 비공개열쇠로 서명된것이 아니거나 암호문이 전송과정에 바뀌였다는것을 알게 된다. 어느 경우에나 수신자는 전문의 내용을 의심하게 된다.

암호화부족점

암호화의 부족점에는 세가지가 있다.

- 잘못된 처리 또는 사람의 오유

• 암호 그자체의 결함
• 힘내기공격

어느 암호화방법이 자기 요구에 제일 알맞는가를 결정할 때 자기 경우의 약점을 반드시 알아야 한다.

잘못된 처리 또는 사람의 오유

암호화방법을 고찰할 때 사람의 실수문제를 론의하는것은 약간 이상할수 있지만 이 문제는 자료의 안전성을 담보하는데서 결정적인 작용을 한다. 어떤 암호화방법들은 다른 방법들에 비하여 열쇠관리가 잘되지 않을수 있다. 암호화방법을 택할 때에는 적당한 방법으로 암호열쇠를 관리하는데 요구되는 정확한 하부구조를 가져야 한다.

비공개열쇠암호를 사용하려고 한다면 호스트들사이에서 열쇠정보를 교환하기 위한 안전한 방법을 가지고 있어야 한다. 비공개열쇠를 단순히 같은 불안전한 통로로 전송하려고 한다면 자료암호화가 그리 좋은것이 못된다. 간단한 열쇠관리는 공개 및 비공개암호열쇠들이 아주 대중적인것으로 된 원인들중의 하나이다. 자료를 전송하는데 쓰려고 하는 불안전한 통로상에서 열쇠정보를 교환하는 능력은 큰 흥미를 끈다. 이것은 열쇠관리를 매우 간소화하는데 송신자는 비공개열쇠를 안전하게 가지고 있고 선택한 어떤 한가지 방법으로 공개열쇠를 전송한다.

열쇠관리를 잘하는것이 중요하다

1940년대에 이전 쏘련은 가장 중요한 자료를 암호화하는데 일회용보충(one-time pad)을 리용하였다. 흐름암호에 대한 절에서도 보았지만 일회용보충을 리용한 암호화를 깬다는것은 수학적으로 불가능하다. 이것은 물론 사용자가 《one-time》의 정의를 리해한다고 본다. 하지만 이전 쏘련은 그렇게 하지 않았다.

암호열쇠들이 짧았으므로 이전 쏘련은 일부 일회용보충열쇠들을 서로 다른 위치들에서 회전시켜 다시 리용하기 시작했다. 전제로 한것은 같은 사용자가 같은 열쇠를 한번이상 리용하지 않는 한 얻어 진 암호문이 충분히 안전하다는것이였다. 명백히 이 가정은 기본을 놓쳤다. 미국은 그중 열쇠모형들을 찾아 내여 암호문으로부터 정확한 전문을 얻어 낼수 있었다.

5년이상이나 미국은 자국내에서의 이전 쏘련의 정탐활동을 추적할수 있었다.

경 고

자료암호화에 리용하는 공개열쇠가 정당한 원천으로부터 받은것이며 공격자가 자기의 비공개열쇠로 바꾸어 놓은것이 아니라는것을 확인하여야 한다. 공격열쇠의 정당성은 전화나 어떤 다른 방법으로 쉽게 인증할수 있다.

암호의 결함

정해 진 형태의 암호화알고리듬에 어떤 결함이 있겠는가를 결정하는것은 비암호전문가에게는 가장 풀기 어려운 문제로 될것이다. 하지만 암호화가 안전한가를 담보하는데서 고려하여야 할 몇가지 문제가 있다.

- 암호화알고리듬을 서술하는 수학식은 공개지식으로 되여야 한다. 비밀성에 의존하는 알고리듬은 쉽게 탈취당할수 있는 결함을 가진다.
- 암호화알고리듬은 철저한 공개검사를 받아야 한다. 누구나 알고리듬을 평가할수 있어야 하며 그 결과를 자유롭게 론의하여야 한다. 이것은 알고리듬의 분석이 제한되지 말아야 한다는것을 의미한다.
- 암호화알고리듬은 일정한 시간동안 공개적으로 리용되여 적당한 분석이 진행되도록 담보하여야 한다. 몇달정도만 리용하여 보아서는 시간적검사를 받았다고 볼수 없다. 많은 사람들이 DES암호화를 믿는 리유의 하나는 그것이 거의 15년동안 가동하고 있었기때문이였다.
- 암호화알고리듬에서는 공개적인 분석에 의하여 약점들이 발견되지 말아야 한다. 거의 모든 암호화알고리듬은 약간의 결함들을 가지고 있다. 이러한 결함들로 하여 그 열쇠를 해득하는데 필요한 시간이 가능한 모든 열쇠조합을 만들어 보는데 걸리는 시간보다 크게 감소될수 있으며 암호문이 쉽게 해득될수 있다.

이러한 간단한 지도방책에 따라 암호화알고리듬의 상대적안전성을 평가할수 있다.

힘내기공격

힘내기공격은 가능한 모든 열쇠조합들을 시도하여 암호문을 푸는 열쇠를 하나 찾아내는 단순한 방법이다. 그러므로 이 공격을 전체열쇠조사라고 한다. 크래커는 열쇠를 해득하려고 하는것이 아니라 적당한 시간내에 가능한 모든 열쇠조합을 시도하려고 한다. 모든 암호화알고리듬들은 힘내기공격에 대하여 취약하다. 앞단락에 한쌍의 중요한 용어가 있다.

첫째는 《reasonable》이다. 공격자는 힘내기공격을 들이대는것이 시간적으로 의미가 있어야 한다고 여긴다. 만일 전체열쇠조사가 VISA백금카드번호를 몇시간안에 풀어 낸다면 공격은 가치가 있는것이다.

다른 한가지는 《vulnerable》이다. 모든 암호화알고리듬들은 힘내기공격을 받을수 있으나 몇가지는 모든 가능한 열쇠결합들을 시도하는데 지내 오랜 시간이 걸린다. 실례로 일회용보충을 리용한 암호화는 힘내기공격을 리용하여 해득할수 있지만 공격자는 그가 죽은 다음에도 몇대의 자손들을 거쳐서야 이 계획을 수행할수 있다. 적당한 일회용보충의 암호화방안을 해득하는데는 현존하는 계산능력을 동원하여 지구가 없어 진다고 볼때까지의 천문학적인 시간이 걸린다. 그래서 힘내기공격실현에 요구되는 시간량은 두가지 요인에 의존하는바 그것은 특정의 열쇠를 시도하는데 얼마의 시간이 걸리는가와 얼마의 가능한 열쇠결합이 존재하는가 하는것이다.

매 열쇠검사에 걸리는 시간은 처리에 리용되는 장치에 달려 있다. 보통의 탁상콤퓨터는 1s에 5개의 열쇠를 검사할수 있다. 암호화열쇠를 깨기 위하여 특별히 만들어 진 장치는 1s에 200개이상의 열쇠를 검사할수 있다. 물론 여러개의 체계들을 결합하면 그보다 더 좋은 결과를 얻을수 있다.

가능한 열쇠조합의 수는 열쇠크기에 직접 비례한다. 크기는 암호학에서 중요한 문제로 된다. 암호열쇠가 클수록 보다 많은 열쇠조합들이 존재한다. 표 9-1은 몇가지 암호화방법들을 그것들의 열쇠크기에 따라 보여 준다. 열쇠크기가 증가할수록 가능한 열쇠조합의 수가 지수함수적으로 증가함을 알수 있다.

표 9-1 암호화방법들과 그것의 열쇠들

암호화방법	열쇠비트수	가능한 열쇠개수
Netscape	40	1.1×10^{6}
DES	56	72.1×10^{6}
Trple DES(2 열쇠)	112	5.2×10^{33}
IDEA	128	3.4×10^{38}
RC4(128bit열쇠)	128	3.4×10^{38}
Triple DES(3 열쇠)	168	3.7×10^{50}
Blowfish	448까지	
AES	128, 192, 256	3.4×10^{38}

이것은 특정의 암호화알고리듬에 대하여 전체열쇠조사를 진행하는데 얼마만한 시간이 걸리는가 하는 물음을 제기한다. 대답은 놀라운것이다. DES암호화(이 장의 DES절에서 론의되는)는 공업규격으로 되였다. 몇년전에 RSA연구소에서는 DES암호문렬을 깨고 그안에 숨겨 진 통보문을 알아 내는데 얼마나 시간이 걸리는가를 알기 위한 도전을 조직하였다.

1997년에는 그 도전이 약 5달만에 완성되였다.

1998년 1월에는 39일만에 완성되였다.

1999년 1월에는 EFF가 이것을 22시간내에 끝낼수 있었다.

EFF는 DES암호화를 힘내기공격하기 위하여 특별히 설계된 장치를 통하여 이것을 진행하였다. 장치의 가격은 대략 25만딸라였다. 이 도전후에 EFF는 《Cracking DES》라는 책을 출판하였는데 여기에는 자기들이 리용한 장치의 설계에 대한 자료들이 완전히 서술되여 있다. 명백히 이것은 얼마만한 열쇠길이가 안전한것으로 간주되는가에 관한 완전히 새로운 견해를 주었다.

정부의 간섭

미련방정부는 국경밖으로의 암호화의 수출과 리용을 규제하고 있다. 이 규제에는 2차세계대전시기에 생겨 났는데 그때는 암호기의 사용을 간첩이나 테로분자들에게만 한한

것으로 생각하였다.

이 규정은 국가안전보장국(NSA)에 의하여 오늘날까지도 여전히 존재하고 있다. NSA는 정부가 관심하는 비밀이 있다고 여겨 지는 모든 통신을 감시하고 풀어야 할 책임을 지니고 있다.

원래의 규정에서는 국경밖으로 수출하거나 사용할수 있는 암호열쇠크기를 제한하였다. 2000년이전에는 최대 40bit크기까지였고 례외로 보다 큰 열쇠크기를 사용하려는 기관은 통상부에 제출하여 허가를 받아야 하였다.

이 모든것은 2000년 1월에 변하였는데 이때 국가에서는 상업적인 암호화제품을 외국에 수출할수 있도록 규정을 바꾸었으며 정부가 암호제품을 먼저 검열한후에 수출하도록 하였다. 다른 나라들도 이와 류사한 규정들을 적용하고 있으며 이 세계적인 추세는 지난 몇년동안에 전자상업의 폭발적인 증대와 관련된다.

좋은 암호화가 필요하다

인증이 제대로 되고 있다면 왜 암호화가 요구되는가? 암호화는 두가지 목적에 쓰인다.

- 자료도청을 막기 위하여
- 자료변경을 막기 위하여

이미 이 장의 평문전송에 대한 절에서 어떻게 대부분의 IP봉사들이 모든 정보들을 평문으로 전송하는가에 대하여 보았다. 이것은 왜 자료를 보호하는데 암호화가 필요한가 하는데 충분한 대답으로 될것이다.

암호화는 또한 자료가 전송도중에 변경되지 않도록 담보할수 있다. 이러한 문제는 중개자공격에 의하여 생기며 자료전송을 파괴하려는 공격자의 능력에 관계된다. 직결목록주문들을 받아 들일수 있도록 구성된 Web봉사기를 가지고 있다고 가정하자. 사용자들은 직결양식들에 써넣으며 그러면 직결양식은 Web봉사기에 평문형식으로 기억된다. 규칙적인 간격으로 이러한 파일들은 FTP나 SMTP를 거쳐서 다른 체계로 전송된다.

만일 공격자가 Web봉사기의 파일체계에 접속할수 있다면 공격자는 이러한 본문파일들을 사전에 변경시킬수 있다. 이때 공격자는 수량이나 제품의 번호들을 변경시킬수 있다. 틀린 주문을 받는 의뢰기는 매우 불행하게 된다. 이 실례에서는 공격자가 파일체계에 접근하고 있다고 가정하고 있지만 망을 통한 중개자공격도 가능하다.

또한 공격자가 자료를 변경시켜 다른 사람의 사업을 혼란시킬수도 있다. 이 정보를 좋은 암호화알고리듬을 리용하여 암호화하면 이러한 공격은 훨씬 힘들어 진다. 왜냐하면 공격자가 암호화된 파일속에 어떤 값이 들어 있는지 알수 없기때문이다. 공격자의 능력이 좋다고 해도 암호를 복호화하는 알고리듬은 자료의 변화를 검출할것이다.

해 결 방 법

인증과 암호화봉사를 제공하여 주는 많은 방법들이 있다. 어떤것은 특정의 제작자에 의하여 제작된 제품들이며 어떤것은 열린 표준들이다. 어느것이 좋은가 하는것은 요구에 따라 다르다. 아래에서 가장 널리 쓰이는 인증 및 암호화방법들을 소개한다.

자료암호화규격(DES)

DES는 미행정부가 리용하는 자료암호화규격이다. 국가표준국(ANSI)과 인터네트기술과제집단(IETF)도 DES를 보안표준으로 받아 들였다. DES는 오늘까지 리용되는 가장 일반적인 비공개열쇠알고리듬이다.

DES의 원래의 규격은 40bit(수출용) 혹은 56bit의 암호화열쇠를 리용한다. 가장 최근의 규격인 3중 DES는 2개 혹은 3개의 서로 다른 56bit열쇠를 리용하여 평문을 세번 암호화한다. 이것은 112bit 혹은 168bit열쇠를 가진 암호문을 만들어 내며 뒤방향호환성을 유지한다. DES는 제3자가 일부 평문과 그것에 따르는 암호문을 안다고 하여도 모든 열쇠를 조사하지 않고서는 그 열쇠를 얻을수 없게 설계되였다. DES의 원래의 규격은 3일동안의 힘내기공격에 의하여 깨여 졌지만 새로운 3중DES규격은 앞으로 몇년동안은 안전한것으로 남아 있을것이다.

개량암호화규격(AES)

개량암호화규격(AES)은 DES를 계승하여 나왔다. AES는 DES의 결함(암호화약점, 열쇠길이의 제한, 장치에 의존하는 응용)을 극복하기 위하여 설계되였으며 앞으로의 기술발전을 위한 틀거리를 제공한다. AES가 2001년 여름까지 완전한 표준으로 설정되지는 않았지만 NIST(국가표준기술국)는 2000년 10월 2일에 Rijndael알고리듬을 DES를 교체할 핵심으로 공포하였다. Rijndael은 가변길이블로크암호이지만 AES에서 실현될 때에는 처음에 열쇠길이 128, 192, 256bit를 취한다.

NIST는 Rijndael이 Pentium급의 기계들뿐아니라 스마트카드들에서도 잘 동작하기때문에 이것을 선택하였다. 또한 가변길이열쇠를 쓸수 있는 능력과 다른 암호화특성들로 하여 NIST는 Rijndael이 AES의 최종평가를 위하여 제기된 5개의 표준들중 가장 좋다고 결정하였다.

수자식증명서봉사기

공개열쇠암호와 비공개열쇠암호에 대한 절에서도 본바와 같이 비공개열쇠는 독특한 전자서명을 만드는데 리용될수 있다. 이 서명은 후에 그것이 인증되였다는것을 담보하기 위하여 공개열쇠로 검증될수 있다. 이러한 과정은 사용자의 신분을 인증하는 매우 강력한 방법을 제공한다. 수자식증명서봉사기는 많은 공개열쇠들의 관리를 위한 중심점을 제공한다. 이것은 매 사용자들이 다른 사람의 공개열쇠를 복사하여 관리하

지 못하게 하여 준다. Lotus Notes봉사기는 수자식증명서봉사기로 동작하는데 사용자들이 자기의 비공개열쇠들을 리용하여 통보문에 서명하게 한다. Notes봉사기는 또한 수신자에게 Notes봉사기가 전자서명을 확인할수 있는가에 대하여 통지한다. 수자식증명서봉사기들은 증명서권한기관(CA)이라고도 하는데 전자서명의 확인을 제공한다. 실례로 만일 Toby가 Lynn으로부터 전자서명이 있는 통보문을 받았지만 Lynn의 공개암호화열쇠를 가지고 있지 못하다면 Toby는 CA로부터 Lynn의 공개열쇠를 받아서 그 통보문이 인증될수 있다는것을 확인할수 있다. 또한 Toby가 Lynn의 전자우편에 응답하려고 하지만 제3자의 도청을 막기 위하여 통보문을 암호화하려고 한다고 하자. Toby는 CA로부터 Lynn의 공개열쇠를 받아서 그 통보문을 Lynn의 공개열쇠를 리용하여 암호화할수 있다.

증명서봉사기는 하나의 서명과 접근조종을 제공하는데 리용될수도 있다. 증명서는 접근을 제한하기 위하여 봉사기에 들어 있는 파일들에 대한 접근조항목록에 첨부될수 있다. 사용자가 파일에 접근하려고 한다면 봉사기는 사용자의 증명서에 접근이 허가되였는가를 확인한다. 이것은 CA가 기관이나 회사의 거의 모든 문서의 보안을 관리하게 한다.

주　　의

Netscape증명서봉사기는 파일준위접근조종을 지원하는 CA의 좋은 실례이다.

CA를 리용하는것의 가장 큰 리득은 그것이 수자식증명서에 대한 공업규격형식인 X.509를 지원하는데 있다. 이것은 기관들사이에서 증명서가 확인되고 정보를 암호화하게 하여 준다. 만일 두 령역사이에 정보를 교환하는 기본방법이 전자우편이라면 CA는 가상사설망을 리용하는것보다 훨씬 더 효과적일수 있다.

IP보안

IP보안(IPSec)은 Cisco체계들에서 많이 리용되고 있는 공개 및 비공개열쇠암호화알고리듬이다. 이것은 열린 표준들의 집합으로서 그리 새로운 형식은 아니다. IPSec는 인증을 실현하고 대화열쇠를 설정하기 위하여 Diffie-Hellman교환을 리용한다. IPSec는 또한 자료흐름을 암호화하기 위하여 40bit DES알고리듬을 리용한다. IPSec는 대화층에서 실현되였으며 따라서 직접적인 응용프로그람지원을 요구하지 않는다. IPSec의 리용은 말단사용자들에게 알기 쉽다.

IPSec의 우점의 하나는 쓰기 편리한것이다. Cisco가 IPSec를 자기의 경로기제품들에 넣은것으로 하여 IPSec는 명백한 가상사설망(VPN)해결책으로 된다. IPSec는 인터네트로부터의 원격망접속에 널리 쓰이고 있으므로 40bit DES알고리듬을 리용하는것은 일반적인 기업리용에 가장 적합하다. 매우 중요한 자료들을 안전하지 못한 통로로 보내야 하는 필요가 있는 기관들은 여러가지 암호화기술들을 선택하는데서 심중하여야 한다.

Kerberos

Kerberos는 또 한가지 인증방법으로서 서로 다른 환경에서 하나의 서명을 제공하기 위하여 설계되였다. Kerberos는 사용자와 봉사들사이의 호상인증과 암호통신을 실현하여 준다. 그러나 보안통표와 달리 매 사용자가 특정의 통과암호를 기억하고 유지하도록 하여 준다. 사용자가 국부조작체계에 인증할 때 국부대행체는 Kerberos봉사기에 인증요구를 보낸다. 봉사기는 체계에 인증하려고 하는 그 사용자에 대한 암호화된 신용증명서를 보낸다. 국부대행체는 그 다음 사용자가 제공하는 통과암호를 리용하여 신용증명서를 해득한다.

만일 정확한 통과암호를 받았다면 사용자는 확인되며 인증표가 제공되여 그는 다른 Kerberos인증봉사에 접근할수 있게 된다. 사용자는 또한 모든 자료들을 암호화하는데 리용될수 있는 암호열쇠모임을 얻는다.

일단 사용자가 확인되면 그는 임의의 Kerberos관련봉사기들이나 응용프로그람들에 대한 인증을 하지 않아도 된다. Kerberos봉사기가 내는 표는 추가적인 망원천들에 접속하는데 필요한 신용증명서들을 제공한다. 이것은 사용자가 여전히 자기의 통과암호를 기억하여야 하지만 망의 모든 체계들에 접근하는데 하나의 통과암호만이 필요하다는것을 의미한다. Kerberos의 가장 큰 우점의 하나는 자유롭게 쓸수 있는것이다. 원천코드는 무료로 내리적재되고 리용될수 있다. 또한 많은 상업적인 응용프로그람들도 있는데 그중 한가지 형태인 IBM의 Global Sign-on(GSO)제품은 Kerberos와 호환가능하며 개선된 관리를 제공한다. 몇해동안 Kerberos에서 많은 보안상의 결함들이 발견되였지만 대부분은 Kerberos V에 의하여 수정되였다.

점대점갱도규약(PPTP)과 계층2갱도규약(L2TP)

암호화기술에 대한 론의는 PPTD와 L2TP를 말하지 않고는 성립할수 없다. Microsoft에 의하여 개발된 PPTP는 점대점규약(PPP)에 기초한 인증과 Microsoft알고리듬에 기초한 암호화를 리용한다. Microsoft는 PPTP를 NT봉사기와 Windows 95/98에 포함시켰다.

암호분야의 많은 사람들은 PPTP를 유치원암호라고 한다. 그것은 이 방법에서의 인증구조와 암호화알고리듬을 깨는것이 비교적 쉽기때문이다. 인터네트에는 PPTP대화안의 통과암호정보를 얻을수 있는 많은 도구들이 있다. 이것은 PPTP가 나온지 4년밖에 되지 않았음을 고려하면 기대에 어긋난다고 볼수 있다. PPTP를 깰수 있는 많은 도구들이 있으므로 그것은 자료를 보호하기 위한 규약으로서는 그리 쓰이지 않는다.

주 의

PPTP의 불안전성에 대한 추가적인 정보를 얻으려면 http://underground.org/를 참고하기 바란다.

계층2갱도규약(L2TP)은 PPTP와 Cisco의 L2F(Layer Two Firewall)의 가장 좋은 부분들을 뽑아서 설계되였다. L2TP는 보통 IPSec와 함께 리용되는데 L2TP는 두점사이의 통로를 만들며 암호화과제는 IPSec가 담당한다. 결과적으로 L2TP는 PPTP에 비하여 다음과 같은 우점들을 가지고 있다.

- L2TP는 프레임중계, X.25, ATM을 포함한 임의의 파케트점대점망우에서 동작할수 있다
- L2TP는 하나의 끝점쌍들사이에 여러개의 련결을 만들수 있다
- L2TP는 자기의 머리부정보를 압축할수 있다
- L2TP는 자기자체의 련결인증을 제공할수 있다(L2TP와 IPSec를 함께 리용할 때에는 필요하지 않다.)

원격접근전화가입사용자봉사(RADIUS)

RADIUS는 여러개의 원격접근장치들이 같은 인증자료기지를 공유하게 한다. 이것은 모든 원격망접근을 위한 관리중심을 제공한다. 사용자가 RADIUS의뢰기(말단접근봉사기와 같은)에 접근하려고 한다면 가입등록이름과 통과암호를 대야 한다. RADIUS의뢰기는 이때 RADIUS봉사기에 이 신용증명서들을 전송한다. 만일 신용증명서들이 옳다면 봉사기는 긍정적인 대답을 주고 사용자는 망에 접근할수 있게 된다. 신용증명서가 옳지 않으면 RADIUS봉사기는 거절답변을 주며 RADIUS의뢰기는 사용자의 련결을 차단시킨다.

RADIUS는 망에로의 원격모뎀접속에 널리 리용되여 있다. RADIUS는 오래동안 3COM, Cisco, Ascend와 같은 제작자들에 의하여 널리 퍼졌다. RADIUS는 또한 방화벽을 통하여 국부망에 접속하려고 시도하는 원격사용자들을 인증하는 방법으로 되고 있다. RADIUS는 Check Point의 방화벽-1과 Cisco의 PIX방화벽에 내장되였다. 방화벽련결에 RADIUS를 리용할 때 가장 큰 약점은 암호화를 포함하지 않는다는것이다. 이것은 RADIUS가 강한 인증을 보장할수 있지만 일단 대화가 설정된 다음에는 자료의 완전성을 담보하지 않는다는것을 의미한다. 만일 방화벽에서 RADIUS인증을 리용한다면 암호화를 제공하기 위한 보충적인 방법이 필요하다.

RSA암호화

RSA암호화알고리듬은 1977년에 리베스트, 샤미르, 아델만에 의하여 만들어 졌다. RSA는 공개 및 비공개열쇠암호에서 사실상의 표준으로 간주되고 있다. 그것은 Microsoft, Apple, Novell, Sun, 지어 Lotus 등의 제품에도 쓰이고 있다. 공개 및 비밀암호체계로서 인증도 실현할수 있다.

RSA가 널리 쓰인다는 사실은 호상리용성과 관련하여 매우 중요하다. 통보문을 만들 때 리용하는 알고리듬과 다른 알고리듬을 쓴다면 그 통보문을 인증하거나 복호화할수 없

다. RSA를 지원하는 제품에서는 넓은 사용자범위에서 정보를 교환할수 있도록 담보한다. RSA는 오래동안 철저한 검토를 진행하였다. 자료를 보호하기 위하여 하나의 알고리듬을 선택할 때 이것은 중요한 인자로 된다. RSA암호는 RSA연구소의 소유이나 지금은 Security Dynamics의 소유하에 있다. RSA알고리듬의 특허는 1983년에 넘겨 져서 2000년에 시간만료되게 되여 있다. RSA연구소는 여전히 특허에 대한 통제를 유지하고 있으나 자기가 만든 기술을 널리 리용하도록 하고 있다. RSA회사는 원천코드를 공개하였으며 비상업적인 목적에 자유롭게 쓸수 있게 되였다.

하쉬알고리듬

전자서명은 비공개열쇠를 리용하여 전체 통보에 서명하는 방법으로 동작한다. 이것은 복잡하며 시간이 많이 든다. 한가지 방법은 하나의 자료요약을 만들고 그다음 그 통보문요약에 비공개열쇠로 서명(또는 암호화)하여(이것을 때로 하쉬라고 한다.) 전체 통보에 서명하는것과 같은 효과를 얻는것이다.

이것은 하쉬알고리듬으로 수행되는데 원래 파일을 입구하여 통보문요약을 만들며 거기에 비공개열쇠로 서명하여 전송한다. 수신자는 서명자의 공개열쇠를 암호화된 하쉬값에 적용하여 수신자의 신분을 검증한다. 수신자는 그다음 송신자와 같은 하쉬알고리듬을 리용하여 원래 파일을 처리하고 원래 하쉬값과 비교한다. 만일 같으면 수신자는 통보가 송신도중에 수정되지 않았다는것을 확인한다.

SHA-1(Secure Hash Algorithm)

SHA-1(안전한 하쉬알고리듬)은 NIST에 의해 제안되여 DSS표준으로 등록되였으며 DES와 함께 전자서명에 리용된다.

1994년에 실현(원래의 SHA에서 몇가지 결함을 수정하여)되였으며 SHA-1은 160bit 통보요약값을 준다. 2000년 10월 12일 NIST는 새로운 AES와 함께 쓰일 SHA에 기초한 3개의 알고리듬을 공개하였다.

SHA-256, SHA-384, SHA-512는 3개의 서로 다른 AES열쇠크기(128, 192, 256bit)로 동작한다.

MD5

1991년 MIT의 로버트 리베스트에 의해 제안되였으며 MD계렬 하쉬알고리듬의 최신판이다. 32bit처리소자에서 동작할수 있게 설계되였으며 MD5는 128bit 요약값을 준다. MD5는 SHA-1보다 빠르지만 더 안전하지는 못하다.

안전한 쉘(SSH)

안전한 쉘은 의뢰기인증을 보장하고 두 체계사이에 다중봉사대화를 보호하는 강력한

방법이다. 핀란드의 대학생 Tatu Ylnen에 의해 제안된 SSH는 UNIX세계에서 널리 쓰이고 있다. 이 규약은 Windows와 OS/2도 내장되였다.

SSH로 동작하는 체계들은 련결요구를 포구 22로 듣는다. 만일 SSH체계로 동작하는 2개의 체계가 련결된다면 매개는 RSA를 리용한 수자식증명서교환을 수행하여 상대방의 신용증명서를 검사한다. 매 사람의 신용증명서가 검증되면 두 체계를 통하여 교환되는 모든 정보를 암호화하기 위하여 3중 DES를 리용한다. 두 호스트들은 통신대화과정에 대방을 인증하며 암호화열쇠를 주기적으로 바꾼다.

이것은 힘내기공격이나 재생공격이 효과가 없게 한다.

SSH는 불안전한 규약을 안전하게 하는 좋은 방법이다.

실례로 telnet와 FTP 대화들은 모두 인증정보들을 평문으로 교환한다. SSH는 이 대화들을 교갑화하여 평문정보가 보이지 않게 한다.

안전한 소케트층(SSL)

Netscape회사에서 만든 안전한 소케트층(Secure Sockets Layer:SSL)은 OSI모형의 대화층에 RSA암호화를 제공한다. 대화층에서 암호화를 진행하여 SSL은 봉사에 독립인 능력을 가지게 된다. SSL은 FTP, HTTP, telnet와 같이 동작하지만 주로 안전한 Web상업에서 많이 리용된다. RSA암호화가 공개 및 비공개열쇠암호화이기때문에 수자식증명서도 지원된다.

이것은 SSL이 봉사기를 인증하고 선택적으로 의뢰기도 인증할수 있게 해준다.

Netscape는 자기의 Web열람기와 Web봉사기제품에 SSL을 포함하고 있다. Netscape는 지어 원천코드를 제공하여 SSL이 다른 Web봉사기플래트홈들에 접속할수 있게 해준다.

Web페지를 만드는 Web전문가는 모든 Web열람기들로부터의 SSL련결요구에 따라 페지를 표시할수 있다. 이것은 직결상업을 비교적 안전한 방법으로 할수 있게 한다.

인터네트기술과제집단(IETF)은 전송층보안규약(TLS)이라고 하는 SSL3.0에 기초한 규격을 검토하고 있다. TLS와 SSL의 차이가 작은 동안은 TLS가 SSL과 함께 쓰이지 않을것이다.

보안통표(Security Tokens)

보안통표는 통표카드(또는 스마트카드)라고도 부르는데 국부의뢰기나 망봉사접근에 리용될수 있는 통과암호생성장치들이다. 물리적으로 통표는 통과암호와 통과암호의 남아있는 시간을 표시하는 LCD현시장치를 가지고 있는 작은 장치이다. 현재의 통과암호의 기간이 끝나면 새로운 통과암호가 발생된다. 이것은 높은 수준의 인증보안을 제공한다. 왜냐하면 약속된 통과암호가 매우 제한된 생명주기를 가지기때문이다. 그림 9-7에 여러

가지 보안통표들을 보여 주었다. 이 통표들을 SecurID카드라고 한다.

보안통표들은 현존 조작체계나 응용프로그람과 직접 인증하지 않는다. 가입등록요구를 인증봉사기에 넘기기 위한 대리자가 요구된다. 례를 들어 방화벽-1은 SecurID를 통하여 들어 오는 의뢰기인증을 지원한다.

그림 9-7. Security Dynamics Technologies에서 생산된 SecurID카드들

인터네트밖의 사용자가 방화벽-1로 보호된 인터네트안의 봉사에 접근하려면 자기의 SecurID통표를 리용하여 방화벽에 인증한다. 방화벽-1은 이 인증을 직접 하지 않고 방화벽우의 대리자가 ACE/Server라고 하는 SecurID인증봉사기에 가입등록요구를 내보낸다.

만일 신용증명서가 정확하면 암호화된 대화를 통하여 대리자에게 옳다는 신호가 오며 사용자는 내부망에 접근할수 있게 된다. 매 보안통표는 ID번호에 의하여 식별된다. ID번호는 매 보안통표를 유일하게 식별한다. ID번호는 또한 매 통과암호를 생성하는데 리용되는 알고리듬을 수정하는데 쓰이며 따라서 여러개의 통표가 같은 통과암호렬을 만들수 없다.

통과암호가 규칙적인 시간간격(보통 60s)으로 만료되므로 보안통표는 처음에 인증봉사기와 동기를 맞추어야 한다.

이러한 형태의 인증은 많은 쓸모가 있다. 우선 사용자는 자기의 통과암호들을 기억할 필요가 없다. 그들은 보안통표로부터 현재의 통과암호를 읽고 이 값을 인증에 리용하면 된다. 사용자는 자기의 통과암호를 규칙적인 시간간격으로 변경시키지 않아도 된다. 왜냐하면 이것은 보안통표에 의하여 자동적으로 실현되기때문이다. 또한 통표가 매 인증에서 리용되는 물리적인 장치이므로 사용자는 보통 자기의 통과암호를 다른 사람에게 줄수 없다. 사용자가 자기의 통과암호를 다른 사용자에게 읽어 준다고 해도 통과암호가 매우 짧은 기간에만 맞기때문에 그 통과암호를 리용할수 없다.

보안통표는 인증을 제공하는 우수한 방법이다. 유일한 약점은 임의의 형태의 대화암호화를 제공하지 못한다는것이다. 그것은 이 기능을 제공하는 조작체계나 응용프로그람에 의존한다. 실례로 이것은 공격자가 telnet대화로 가장하고 들어 온다면 인증정보를 평

문으로 읽을수 있다는것을 의미한다. 그러므로 주어 진 통과암호의 제한된 생명주기는 이러한 정보를 리용하기 어렵게 한다.

인더네트규약을 위한 단순열쇠관리(SKIP)

SKIP는 대화층에서 동작한다는 점에서 SSL과 비슷하다. SSL과 마찬가지로 SKIP는 IP봉사가 암호화를 지원하는가에 관계없이 그 봉사를 지원하는 능력을 가진다. 이것은 두 호스트사이에서 동작하는 여러개의 IP봉사들을 가지고 있는 경우에 매우 쓸모있다.

SKIP와 SSL과 다른점은 대화층사이에서 설정 및 열쇠의 교환을 위한 사전통신이 필요 없는것이다. Diffie-Hellman의 공개 및 비밀알고리듬은 공유된 비공개열쇠를 생성하는데 쓰인다. 이 공유된 비공개열쇠는 IP파케트에 기초한 암호화와 인증을 제공하는데 쓰인다. SKIP는 자료의 암호화에 매우 효과적일뿐아니라 VPN의 성능을 개선하는데 이것은 매 대화의 완전성을 유지하기 위한 공유된 비공개열쇠를 장기적으로 보호하는데 기초하고 있다.

SKIP는 SSH에서와 같이 새로운 열쇠값들을 련속적으로 생성하지 않는다. 그러므로 열쇠가 적당히 보호되지 않으면 SKIP암호화는 취약하다.

요 약

이 장에서는 인증이 왜 중요하며 인증을 리용하지 않을 때 어떤 종류의 공격이 있을수 있는가에 대하여 보았다.

또한 암호화에 대하여서와 공개 및 비밀알고리듬의 차이에 대하여 보았다. 마지막으로 지금 쓰이고 있는 많은 인증 및 암호화방법들에 대하여서도 보았다.

다음장에서는 가상사설망(VPN)을 만드는데 암호화가 어떻게 쓰이는가 하는것을 취급한다.

제１０장. 가상사설망

인터네트의 도입은 많은 좋은 점과 함께 많은 론쟁거리를 가져 왔다. 가상사설망(VPN)은 WAN의 비용을 감소시키며 경계선보안을 강화하기 위하여 진행되였다. 흥미 있는것은 VPN기술을 배비하는데 앞장 서는것이 금융기관들, 무역회사 그리고 공격 받을 위험이 큰 기업체들이라는것이다. 금융기관들과 기업체들은 자기들의 망범위를 확대하기 위하여 VPN들을 받아 들이고 있다.

VPN기초

가상사설망대화는 인터네트망과 같은 공공망에서의 인증되고 암호화된 통신통로이다. 망이 불안전하다고 보아 지므로 전송되는 자료를 보호하기 위하여 암호화와 인증이 리용된다. VPN은 봉사독립인데 이것은 두개의 호스트(Web, FTP, SMTP 등)들사이에 교환되는 모든 정보들이 이 암호화된 통로를 통하여 전송된다는것을 의미한다.

그림 10-1은 VPN구성의 전형적인 실례를 보여 준다. 그림은 인터네트에 련결된 두개의 서로 다른 망들을 보여 준다. 이 두 망들은 정보를 교환하려고 하지만 교환하려는 정보가 비밀이므로 안전하게 교환하려고 한다. 이 정보를 보호하기 위하여 두 싸이트사이에 VPN이 설치된다.

VPN을 설치하기전에 두개의 망은 다음과 같은것을 하여야 한다.

- 매 싸이트는 망경계에 VPN가능한 장치를 설치하여야 한다. 이것은 경로기나 방화벽 또는 VPN전용장치일수도 있다.
- 매 싸이트는 다른 싸이트가 리용하는 IP부분망주소를 알고 있어야 한다.
- 두 싸이트들은 같은 인증방법을 가지며 필요하다면 수자식증명서를 교환하여야 한다.
- 두 싸이트들은 같은 암호화방법을 가지며 필요하다면 암호화열쇠를 교환하여야 한다.

그림 10-1에서 VPN 통로의 매끝에 있는 장치들은 인터네트련결에 쓰이는 경로기들이다.

만일 Cisco경로기가 있다면 Diffie-Hellman의 인증과 40bit DES암호화를 제공하는 IPSec를 지원할수 있다.

망 A의 경로기는 192.168.2.0부분망으로 가는 모든 나가는 자료흐름이 DES를 리용하여 암호화되도록 구성되여야 한다. 이것을 원격암호화령역이라고 한다. 망 A의 경로기는 또한 망 B의 경로기에서 받은 임의의 자료가 복호화되여야 한다는것을 알아야 한다. 마찬가지로 망 B의 경로기는 부분망 192.168.1.0으로 향하는 모든 자료흐름을 암호화하며 망 A의 경로기로부터 받은 임의의 응답을 복호화할수 있게 구성되여야 한다.

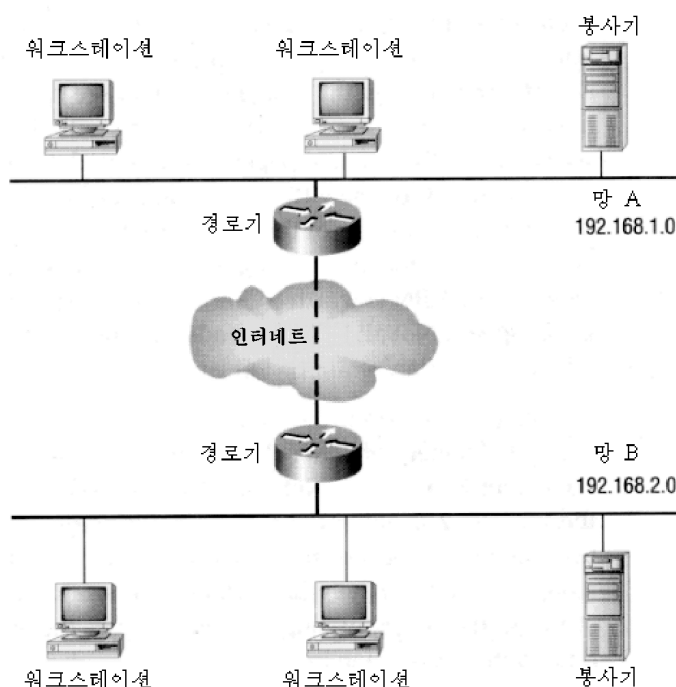



그림 10-1. 두 인터네트싸이트들사이의 VPN의 실례

인터네트의 모든 다른 호스트들에 전송된 자료는 명백히 평문으로 전송된다. 암호화되는것은 이 두 부분망들사이의 통신뿐이다.

주 의

VPN는 두개의 암호화령역들사이의 통신대화들만을 보호한다. 여러개의 VPN들을 설치할 때에는 여러개의 암호화령역을 정의하여야 한다.

어떤 VPN구성에서 두 경로기들사이에 위치한 망분석기는 두 경로기의 대변부의 원천 및 목적지IP주소를 리용하는 모든 파케트들을 현시할수 있다. 그러나 자료를 전송한 호스트의 IP주소를 볼수 없을뿐아니라 목적지호스트의 IP주소도 볼수 없다. 이 정보는 원래 파케트안에 들어 있는 실제적인 자료와 함께 암호화된다. 원래의 파케트가 암호화되면 경로기는 자기의 IP주소를 원천주소로 하고 원격경로기의 목적IP주소를 리용하는 새로운 IP파케트안에 이 암호문을 교갑화한다. 이것을 통로뚫기(tunneling)라고 한다. 이렇게 하면 모든 파케트들이 이 두 경로기들의 IP주소를 리용하므로 공격자는 VPN을 통과하는 자료흐름이 공격할 가치가 있는것인지 추측할수 없게 된다. 모든 VPN방법들이 이 기능을 유지하는것은 아니지만 이 기능은 쓸모 있는것이다.

두 경로기사이에 가상적인 통로가 있으므로 인터네트의 사설주소공간을 리용하는것에 추가적인 리득을 얻게 된다. 례를 들면 망 A의 호스트는 망주소변환이 없이도 192.168.2.0망우의 호스트에 자료를 전송할수 있다. 그 리유는 경로기들이 이 자료가 통로을 따라 전송될 때 이 머리부정보를 교갑화하기때문이다. 망 B의 경로기가 그 파케트

를 받으면 교갑파케트를 풀고 원래의 파케트를 복호화하며 그 자료를 목적지호스트에 전송한다.

VPN은 또한 플래트홈과 봉사에 독립이라는 우점도 가지고 있다. 안전한 통신을 진행하기 위하여서는 워크스테이션은 암호를 지원하는 쏘프트웨어를 리용하지 않아도 된다. 이것은 자료흐름이 두개의 경로기사이를 통과할 때 자동적으로 실행된다. 이것은 평문으로 전송되는 SMTP같은 봉사도 목적지호스트가 원격암호화령역안에 있다면 안전한 방식으로 리용될수 있다는것을 의미한다.

VPN의 리용

VPN들이 널리 리용되고 있지만 그것들은 두개의 특정한 응용프로그람들에서만 리용되고 있다. 그것들은 다음과 같다.

- 전화접속모뎀풀의 교체
- 전용WAN련결의 교체

VPN은 이 기술들을 완전히 또는 특정한 경우에만 대신할수 있다.

이렇게 응용이 제한되는것은 VPN을 구성하는데 필요한 수동적인 작업량에 크게 관련된다. 기술이 발전되는데 따라 이 과정은 보다 가변적인것으로 될것이다. 실례로 두개의 IPSec호환인 두 경로기는 SMTP자료흐름을 전송하기전에 가변적으로 련결설정하고 열쇠들을 교환할수 있다. 전송과정이 끝나면 VPN은 해체된다. 이 기술은 현재 널리 쓰이지는 못하지만 앞으로 가능하게 될것이다.

모뎀풀교체

모뎀풀은 항상 망관리자들을 괴롭히는것으로 되여 왔다. 안정한 해결책이 준비되여 있지 않은것으로 하여 이것들은 보통 많은 비용이 들므로 작거나 중간크기의 회사들에서는 큰 부담으로 된다.

원격사용자들에게 있어서 VPN방법은 유지비용을 쉽게 줄일수 있게 한다. 많은 전화선들을 유지하지 않아도 된다. 또한 새로운 모뎀표준이 나올 때마다 자기의 하드웨어를 갱신하거나 ISDN과 같은 새기술을 지원하기 위하여 전화선들을 갱신할 필요는 없다.

모든 들어 오는 접근은 회사가 인터네트우의 기업을 위하여 이미 가지고 있는 련결인 인터네트련결을 통하여 관리된다.

접근비용은 보다 더 눅을수 있다. 실례로 많은 기관들은 종업원들이 료금을 내지 않고 망에 원격으로 접근할수 있도록 하기 위하여 번호 800을 가지고 있다. 이것은 기관에 큰 부담을 줄수 있다. 왜냐하면 800번을 리용하는 분당료금이 직접 호출하는 비용의 2배로 될수 있기때문이다. 대부분의 ISP의 료금은 매달 20딸라이거나 그이하이다. CompuServe와 같은 큰 ISP들은 지역전화번호들을 국제적으로 제공할수도 있다. 서투른 원격접근사용자들에게 있어서는 800번의 료금을 지불하는것보다 하나의 ISP구좌에 지불

하는것이 훨씬 효과적이다.

이렇게 하면 하부구조비용을 줄이는 한편 말단사용자유지비용도 줄일수 있다. 가장 일반적인 원격접근방조문제는 말단사용자가 망설정을 구성하고 망에 련결하도록 도와 주는것이다. 만일 사용자가 처음으로 한 ISP에 전화가입을 하려고 한다면 이것은 접근을 제공하는 그 ISP에 의하여 제공될수 있다. 사용자가 인터네트밖의 자원에 접근할수 있지만 내부자원에 련결할 문제들을 가지고 있다면 기관의 방조가 동반되여야 한다. 이것은 요구되는 지원의 범위를 크게 제한한다.

일러두기

방화벽을 선택할 때 말단사용자에게 원격VPN접근을 제공할것인가를 고려하여 보아야 한다. 대부분의 방화벽프로그람묶음들은 특별한 의뢰기쏘프트웨어를 제공하므로 말단사용자는 그 방화벽에 하나의 VPN을 만들수 있다.

말단사용자들에게 원격VPN접근을 제공할것인가를 결정할 때 고려하여야 할 몇가지 결함들이 있다. 첫째로, 원격워크스테이션의 완전성이다. 인터네트상에 L0pht의 Netcat와 Dead Cow의 Cult와 같은 침입도구들이 무상으로 제공되고 있으므로 원격워크스테이션이 손상될수 있는 가능성이 매우 크다. 대부분의 ISP들은 전화가입사용자들을 위하여 어떤 형태의 방화벽도 제공하지 않는다. 이것은 전화가입된 체계들이 공격을 쉽게 받을수 있다는것을 의미한다. 원격의뢰기에는 공격자가 침투하여 VPN통로을 리용하여 내부자원을 공격할수 있다.

또다른 결함은 보다 리론적이다. VPN이 망에 접근하도록 하는것은 자기의 방화벽을 통하여 또 하나의 구멍을 뚫을것을 요구한다.

매개의 열린 구멍은 공격자에게 더 많은 구멍을 뚫을수 있는 길을 주는것으로 된다.

실례로 자기 망에 대한 안전한 암호화된 접근을 제공하는 PPTP에 의존하는 NT사용자들은 NT봉사기에서 동작하는 PPTP봉사에 약점이 발견되면 공격 당할수 있다.

PPTP봉사기에 틀린 파케트길이값을 가진 하나의 PPTP대화시작요청을 보냄으로써 공격자는 봉사기를 파괴할수 있다. 이것은 PPTP봉사기와 그 체계에서 동작하는 임의의 다른 봉사도 정지시킨다.

전용WAN련결의 교체

그림 10-1에서 본바와 같이 VPN은 인터네트상에서 두개의 지리학적으로 떨어 져 있는 망을 련결하는데 리용될수 있다. 이것은 두개의 싸이트가 멀리 떨어 져 있을 때 실례로 하나의 회사가 서로 다른 두 도시에 각각 하나의 사무소를 가지고 있을 때 매우 유익하다. 세계를 가로 지르는 전용선을 늘일 대신에 매개 싸이트는 지역ISP에 련결하면 된다. 그러면 인터네트가 이 두 망들을 련결하는 중추망으로 리용될수 있다.

VPN련결은 두 싸이트가 서로 가까울 때에도 유익하다. 실례로 자기의 기업상대와 정보를 교환하려고 하지만 전용련결을 가지기는 어렵다면 이미 구축된 인터네트련결을 통과하는 VPN통로가 그 해결책으로 될수 있다.

체계용량검열표

만일 의뢰기에 자기 망에로의 VPN접근을 제공하고 있다면 체계용량에 주의를 돌려야 한다. 여기에 알아 두어야 할 몇가지 문제들이 있다.

- 동시에 들어 오는 사용자가 얼마나 되는가?

  사용자들이 많을수록 용량이 커야 한다.

- VPN의뢰기들이 언제 망에 원격으로 련결할것인가?

  대부분의 원격VPN접근이 보통의 사업시간에 발생한다면 보다 빠른 인터네트련결과 빠른 하드웨어가 요구된다.

- 어떤 봉사들에 의뢰기들이 접근하고 있는가?

  만일 원격VPN접속이 파일공유와 같은 대역너비집약적인 응용프로그람들에 대한것이라면 역시 보다 빠른 인터네트련결과 보다 빠른 하드웨어가 요구된다.

- 어떤 종류의 암호화를 쓰려고 하는가?

  만일 원격VPN접속이 3중DES와 같이 긴 열쇠알고리듬을 리용하면 보다 빠른 암호화하드웨어가 필요하다.

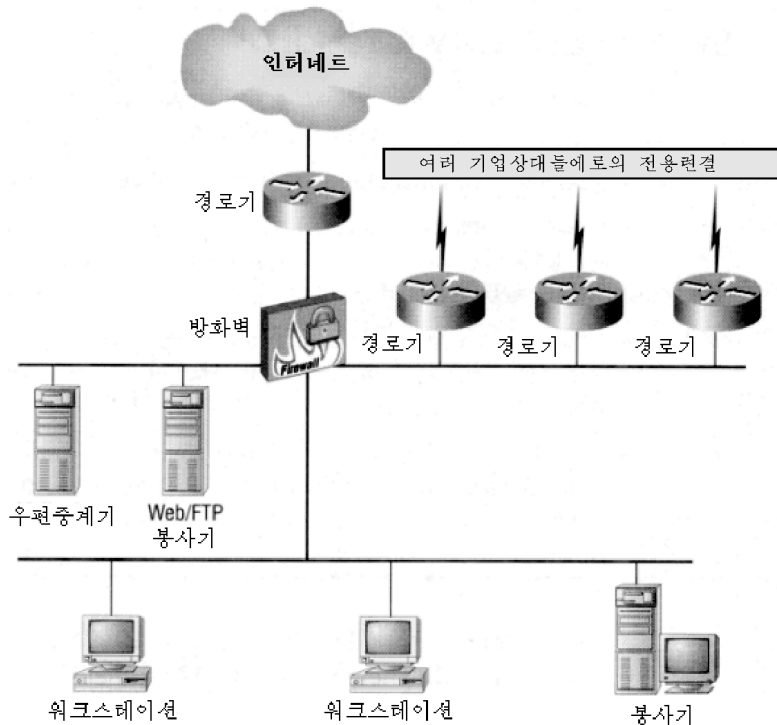



그림 10-2. 중요한 정보들을 지키기 위하여 전용련결을 리용하는 망

그림 10−2의 망을 고찰하자. 여기에는 방화벽으로 보호된 내부망이 있다. 또한 Web 봉사기와 SMTP중계기를 가지고 있는 DMZ토막이 있다. 또한 많은 전용Tl선들에 대한 보안을 관리하기 위하여 방화벽에 하나의 보충적인 망기판을 가지고 있다. Tl회선들은 기관을 여러 기업상대들에게 련결하며 중요한 정보가 인터네트로 나가지 못하도록 하기 위하여 리용된다. 이 중요한 정보들은 전자우편이나 FTP에 의해 전송될수 있다.

이 구성은 표면상으로 아주 명백한것 같지만 많은 잠재적인 문제점들을 가지고 있다. 첫째로, 경로조종문제이다. 방화벽은 이 매개의 원격망들에 대한 경로정보로 프로그람화되여야 한다. 그렇지 않다면 방화벽은 자기의 기정의 경로설정에 따라 이 자료흐름을 인터네트에로 전송하게 된다. 이 경로항목들이 동적으로 설정되므로 하나의 원격망이 경로정보나 부분망을 변화시키면 기관의 망은 어떻게 갱신될것인가?

만일 RIP를 리용하면 그것은 제3장에서 보다싶이 안전하지 못한 경로조종규약이다. 열린최단경로우선규약(OSPF)은 보다 좋은 선택으로 되지만 그것은 련결의 다른 끝에 있는 장치에 의존하므로 OSPF를 선택하지 못할수도 있다.

IP주소와 관련하여서도 문제가 있다. 원격망들중 하나가 사설주소공간을 가진 NAT를 사용한다면 어떻게 되겠는가?

이 체계들중 하나에서 DNS보기를 실행한다면 사설IP주소가 아니라 공개IP주소를 받을것이다. 이것은 추가적인 경로조종문제를 제기하며 이 체계들을 위하여 DNS항목들을 따로 만들어야 한다는것을 의미한다. 또한 만일 두개 또는 그이상의 원격망들이 같은 사설주소공간을 리용하고 있다면 어떻게 되겠는가? 그러면 그 련결의 끝에 있는 경로기에서 NAT를 실행시켜 자기호스트들이 2개의 망들을 구별할수 있게 하여야 한다.

여기에는 또한 책임문제도 있다. 만일 기관의 원격기업상대들중의 하나에 위치한 공격자가 다른쪽의 원격기업상대를 공격한다면 어떻게 되겠는가? 그 기관은 이 공격에 필요한 매체를 제공한것으로 된다.

법적으로 자신을 변호할수는 있지만 이것은 자기의 사업신용을 떨어 뜨린다.

자기의 원격기업상대들과의 련결을 VPN으로 교체함으로써 우에서 본 모든 문제점들을 해결할수 있다. 자기의 자료흐름의 완전성을 담보할수 있는 한 여러개의 VPN을 관리하는것은 여러개의 전용회선들을 관리하는것보다 훨씬 더 쉽다.

원격의뢰기접근에서와 마찬가지로 VPN자료흐름을 허용하기 위하여서는 방화벽을 통하여 하나의 구멍을 열어 놓아야 한다. 강한 보안은 공격자가 이 구성을 리용할 기회를 크게 감소시키지만 그것은 어쨌든 경계선보안에서의 하나의 구멍이다.

VPN제품의 선택항목

자기가 리용할 VPN제품을 선택할 때 여러가지 문제들을 고려하여야 한다.

- 강한 인증
- 충분한 암호화
- 규격에 맞는가？
- 다른 망봉사들과의 통합

만일 어떤 전용의 싸이트를 련결하기 위하여 하나의 VPN을 설치한다면 선택안들은 제한될수 있다. 실례로 Novell의 방화벽제품인 BorderManager는 VPN련결을 지원한다. 문제는 VPN이 독점적이라는것이다. 이것은 Border Manager방화벽을 가진 VPN을 만들려면 VPN통로의 다른 끝에 다른 BorderManager방화벽을 설치하여야 한다는것을 의미한다. 만일 특정의 원격망과 통신하려고 VPN을 설치한다면 그 망이 어떤 VPN묶음을 리용하는가를 알아야 한다. 그 다음에야 자기가 어떤 제품을 선택할것인가를 결정할수 있다.

강한 인증

강한 인증이 없이는 VPN통로의 다른 끝에 있는 체계가 누구인지 정확히 결정할수 없다. 제9장에서 고찰한 Diffie-Hellman알고리듬은 그 통로의 끝점을 확인할 때 쓸수 있는 인증방법이다.

여기서는 공개열쇠들의 교환을 통하여 비밀열쇠들을 공개한다. 그렇게 되면 어떤 또 하나의 수단을 통하여 비밀정보를 교환할 필요가 없다.

일러두기

만일 인터네트상에서 공개열쇠를 교환할 때 믿음성 있는 증명서권한을 리용하지 않는다면 전화나 팍스와 같은 다른 방법들을 통하여 열쇠값들을 확인하여야 한다.

충분한 암호화

《충분하다》는것은 《강하다》는것을 의미하지 않는다. 암호화방법을 선택하기전에 어떤 준위의 보안이 요구되는가를 결정하여야 한다. 실례로 인터네트상에서 중요하지만 꼭 비밀은 아닌 자료를 주고받을 때에는 40～56bit DES암호면 충분하다. 재정자료나 그 밖의 중요한 자료를 보낼 때에는 3중DES와 같은 강한 암호를 써야 한다.

옳은 암호화준위를 선택하여야 하는 리유는 성능과 관련된다. 리용하는 암호화알고리듬이 강할수록 암호화와 복호화과정에 많은 시간이 요구된다. 실례로 56K회선을 통하여 인터네트에 련결된 두망이 3중DES를 리용한다면 응용프로그람의 한계시간을 보장할수 있도록 충분히 빨리 자료를 통과시킬수 없다.

열쇠를 쓰기전에 어떤 크기의 열쇠가 필요한가를 생각하여 보아야 한다.

리용하는 열쇠의 형태도 성능에 영향을 준다. DES와 같은 비밀열쇠암호화는 빠르기때문에 VPN들에서 많이 쓴다. 그러나 RSA와 같은 공개 및 비밀열쇠암호는 같은 크기의 열쇠를 쓰는 비밀열쇠암호알고리듬보다 10～100분의 1정도로 느리다. 따라서 공개 및 비밀열쇠암호화의 열쇠관리는 더 많은 처리시간을 요구한다. 많은 VPN제품들은 초기에 열쇠를 교환하기 위하여 공개 및 비밀열쇠알고리듬을 리용하며 그다음 통신에는 모두 비밀열쇠암호를 리용한다.

일러두기

제9장에서 고찰한 힘내기공격시간을 추정하여 VPN에서 리용할 암호화열쇠의 크기를 결정하는데 리용할수 있다.

규격에 맞는가

제9장에서 왜 암호체계에 대하여 공개적인 철저한 검사를 진행해야 하는가에 대하여 보았다. VPN에 쓰이는 암호화방법을 선택할 때에도 마찬가지이다. 알고리듬을 충분히 검사하여 큰 약점이 없는가를 조사하여야 한다. 실례로 DES에서 유일한 결함은 열쇠의 크기가 작은것이다. 이것은 리용되는 열쇠의 수를 증가시킬수 있는 3중DES를 리용하여 극복할수 있다.

또한 VPN제품이 다른 VPN방법들과 호환되는가를 확인하여야 한다. 이 절의 앞에서 언급한바와 같이 Novell의 BorderManager는 다른 BorderManager체계들을 가진 VPN련결들만을 실현할수 있다. 이것은 통로의 다른 끝에서 제품의 선택을 크게 제한한다. 만일 방화벽대책으로서 BorderManager를 리용하고 그후에 원격기업상대에로의 VPN을 실현하려고 한다면 이 요구를 실현하기 위하여 따로 대책을 세워야 한다.

다른 망봉사들과의 통합

최신의 VPN실현은 방화벽사용자등록부 그리고 감시Web와 같은 다른 봉사들과 통합할 능력을 가진다. Check Point의 VPN-1은 전체 Check Point관리묶음으로 완전히 통합되였으며 이로 하여 보안통합뿐아니라 주소변환, 대역분배 등도 실현할수 있게 해준다. VPN련결의 인증을 중심에서 관리하는 능력은 매 련결이 얼마의 대역너비를 가지고 있는가를 조종하는것과 마찬가지로 강력한 특징으로 된다.

물론 리상적인 VPN실현은 서로 다른 제작자들의 제품들도 통합할수 있다. 지금까지는 새로운 제품들이 LDAP나 3중DES와 같은 공업규격들을 포함하고 있었지만 통합에 성공하지는 못하였다.

Microsoft는 그러한 실례의 하나이다. 그들은 Windows 2000안에 VPN실현을 포함하고 있다. 물론 그 우점은 암호화와 인증기술을 능동등록부와 통합한것이다. 일부 제작자들(Check Point와 같은)은 자기의 VPN제품들을 Microsoft VPN과 혼합하여 하나의 중심적으로 정의된 VPN방책이 Microsoft와 특정제작자의 VPN접근점에 동일하게 적용되도록 하고 있다. 또한 능동등록부가 LDAP-적응이므로 제3자의 VPN들은 능동등록부에 보관된 사용자구좌정보의 VPN허가에 기초할수 있다.

VPN제품의 종류

VPN제품의 종류에는 여러가지가 있다. 이것들을 크게 3가지 류형으로 갈라 볼수 있다.

- 방화벽형VPN
- 경로기형VPN
- 전용의 쏘프트웨어나 하드웨어

어느 종류를 선택하겠는가 하는것은 자기의 요구와 이미 구입한 설비에 의존한다.

방화벽형 VPN

가장 널리 쓰이는 VPN실현은 방화벽통합이다. 사람들이 대체로 방화벽을 자기 망주변에 설치하고 싶어 하므로 이 장치가 VPN련결을 지원하도록 하는것은 자연스러운 확장으로 된다. 이것은 관리의 중심점을 제공하며 기판의 방화벽보안방책과 통파시키려고 하는 자료흐름사이에 직접적인 접촉을 실현한다.

유일한 결함은 성능문제이다.

바쁜 인터네트회선을 가지고 있다면 그리고 강한 암호화를 가지는 여러개의 VPN을 리용하려고 한다면 이러한 봉사를 진행하려고 할 때 체계에 과부하를 주게 된다.

이것은 대체로 일반적으로 제기되는 문제는 아니지만 성능과 규모를 고려하여 VPN통로을 어디서 끝마치겠는가를 결정하여야 한다.

방화벽-1과 같은 일부 방화벽들은 처리기부하를 감소시키기 위하여 암호화기판들을 지원한다. 암호화기판은 표준PCI확장홈에 맞으며 암호화와 복호화를 다 취급한다.

그러나 이 기판들을 리용하려면 자기의 PCI확장홈들이 망기판들에 의하여 쓰이고 있지 않는가를 확인하여야 한다.

경로기형VPN

또 한가지 선택은 인터네트경계선경로기이다.

이것은 인터네트에 련결하기 위하여 설치하는 또 하나의 장치이다. VPN을 자기의 경계선경로기에서 끝나게 하면 자료흐름이 방화벽에 도착하기전에 그것을 복호화할수 있게 된다.

처리기부하가 문제로 되므로 많은 경로기들은 전용집적회로(ASIC)를 리용한다. 이것은 경로기에 특정의 과제를 담당한 처리기들을 배속시키므로 경로기에 과부하가 걸리지 않게 된다.

경로기형VPN실현의 유일한 약점은 보안문제이다.

일반적으로 경로기들은 방화벽에 비하여 매우 약한 경계선보안을 제공한다. 공격자가 VPN통로의 다른쪽에서 오는것처럼 보이는 거짓자료를 경로기로 통파시킬수 있다. 이것은 공격자가 인터네트의 다른 위치에서는 보이지 않게 봉사에 접근할수 있다는것을 의미한다.

전용하드웨어 또는 쏘프트웨어

만일 이미 방화벽과 경로기를 구입하였지만 VPN능력을 지원하지 않는다 하여도 모든것을 잃은것은 아니다. VPN련결을 만들기 위한 전용의 하드웨어나 쏘프트웨어를 여전히 쓸수 있다. 실례로 DEC의 AltaVista Tunnel은 원격망과 원격사용자VPN에로의 통로를 지원하는 우수한 제품이다. 이것은 독립적인 제품이기때문에 임의의 현존방화벽에서도 동작할수 있다.

전용실현의 가장 큰 약점은 추가적인 보안관리점들이 생기는것이다. 만일 장치가 방화벽바깥에 놓여 있다면 경로기에서와 같은 속임수문제들을 가지는것으로 된다. 장치를 방화벽안에 넣으면 자기의 방화벽보안방책을 리용하는 접근을 관리할수 없게 된다. 대부분의 VPN실현은 원래의 파케트를 그대로 암호화한다. 이것은 자료흐름조종결정을 하는

데 IP머리부정보가 더이상 쓸모가 없다는것을 의미한다. 통로의 한끝에서 다른 끝으로 지나 가는 모든 자료흐름은 같은 교갑화파케트머리부를 리용한다.

이것은 방화벽이 그 통로에서 교갑화된 SMTP와 telnet대화사이를 구분할수 없다는것을 의미한다. 통로의 끝으로 통과시키려는 자료흐름의 형태를 조정하기 위한 도구를 제공하려면 전용VPN장치에 의거하여야 한다.

또다른 VPN

모든 원격접근문제가 충분한 기능을 가진 VPN을 요구하는것은 아니다. 어떤 응용프로그람들은 이미 강한 암호화와 인증을 제공한다. 실례로 Lotus Notes의 사용자에게 있어서 Notes ID파일은 사실상 비밀암호화열쇠이다. 이 열쇠는 수자식증명서를 만드는데 리용될수 있는데 이것은 통과암호인증과 함께 자기가 누구인가를 확인하는데 리용된다.

Lotus Notes는 또한 망을 통하여 전송하는 정보를 암호화한다. Lotus Notes의뢰기의 기본차림표에서 File → Tools → User Preferences → Ports를 선택하면 그림 10-3의 User Prefrences화면을 얻을수 있다.

Encrypt network data의 검사칸을 선택하여 우에서 강조된 통신포구를 통하여 전송되는 모든 자료를 암호화할수 있다. 그림 10-3에서 모든 TCP/IP자료흐름은 암호화될것이다.

원격망접근이 Lotus Notes 응답으로 제한된다면 방화벽을 통하여 하나의 포구를 열어서 Lotus Notes가 모든 인증과 암호화를 관리하게 할수 있다. Lotus Notes봉사기를 인터네트상에 열린채로 남겨 두지 않으려면 모든 들어 오는 대화들이 방화벽에서 먼저 인증되도록 할수 있다(방화벽이 이 기능을 가지고 있다면). 이것은 방화벽에 인증될 때까지 Lotus Notes봉사기는 접근불가능으로 남아 있게 된다는것을 의미한다. 방화벽인증에 통과되면 봉사기자료에 접근하기전에 또 Notes인증을 통과하여야 한다.

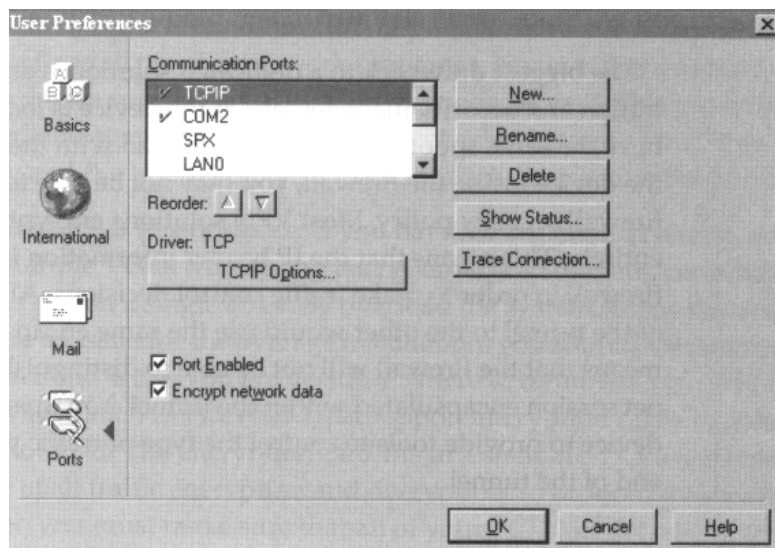



그림 10-3. Lotus Notes의 User Preferences화면

주 의

Lotus Notes는 모든 의뢰기-봉사기, 봉사기-봉사기통신에 TCP포구 1352를 리용한다.

매우 적은 제품들만이 자기의 인증 및 암호화기능을 가지고 있다. 일부는 추가적인 망자원에 접근할수 있게 한다. 실례로 Citrix의 WinFrame과 MetaFrame제품은 WindowsNT 조작체계에 기초한 말단봉사기능력을 제공한다. 또한 괜찮은 인증과 암호화를 제공한다. 이것은 인터네트상의 사용자가 암호화된 대화를 통하여 Citrix봉사기에 접근하기 위하여 Citrix의뢰기를 리용할수 있다는것을 의미한다. 일단 봉사기에 련결되면 사용자들은 체계관리자가 접근을 허가한 임의의 내부응용프로그람들에 접근할수 있다.

이 방법의 가장 큰 결함은 련결을 시작하기 위하여서는 의뢰기에서 특별한 쏘프트웨어를 돌려야 한다는것이다. 그러면 실제적인 진짜 VPN의 봉사기독립성은 더는 존재하지 않는다. 그러나 Citrix와 같은 회사들이 자기의 제품이 만능적으로 접근가능하도록 노력을 기울이고 있는 결과 문제는 달라 지고 있다.

실례로 WinFrame과 MetaFrame의 최신판들은 더이상 전문화된 의뢰기의 리용을 요구하지 않는다. 지금은 누구나 Netscape와 Internet Explorer의 최신판을 지원하는 Web열람기접속을 리용할수 있다.

일러두기

열람기접속은 훌륭한 원격문제해결책으로 될수 있다. 망관리자는 Web봉사기를 통하여 접속쏘프트웨어와 구성파일을 준비하면 된다. 그러면 원격사용자들은 요구되는 쏘프트웨어(약 300KB)를 내리적재하여 자기가 좋아 하는 Web열람기를 리용하여 Citrix봉사기에 련결할수 있다.

VPN의 설치

두개의 원격망사이에 VPN을 형성하기 위하여 제7장에서 론의한 방화벽-1제품에로 되돌아 가보자. 우리가 방화벽-1을 론의하고 있을 때에는 VPN을 설치하는데 필요한 모든 단계들이 다른 제품들의 설치와 류사하다. 목적은 구성과정에 어떤것이 필요한가를 인식시키는것이다.

제7장에서 언급한바와 같이 방화벽-1은 많은 VPN선택안들을 지원한다. 여기에는 SKIP와 IPSec 그리고 방화벽-1의 전용알고리듬들이 포함된다. 이 실례에서는 SKIP가 IPSec보다 더 좋은 인증을 제공하며(비록 추세는 SKIP능력을 IPSec에 통합시키지만) 규격으로 접수되였으므로 SKIP를 리용하기로 한다. 그것은 또한 완전한 통로뚫기를 지원하는데 이것으로 하여 SKIP가 사설주소공간환경에서 리용될수 있게 한다.

방화벽의 준비

주 의

방화벽-1에 대하여 잘 모르면 제7장을 복습하면 된다.

이 절에서는 조종되는 인터네트접근을 제공할수 있는 능력을 가진 방화벽을 가지고 있다고 가정한다. 이 과정에 방화벽방책이 최소의 규칙들만을 가지고 있다는것을 알수 있다. 이 실례에서 그것은 간단성을 위하여 가정되였다. 규칙모임은 변할수 있으며 모든 요구되는 방책들을 포함하여야 한다.

주 의

암호화규칙들은 방책을 편집할 때 맨앞에 넣어 우선적으로 취급하여야 한다.

VPN도식

그림 10-4는 우리가 만들 VPN의 망그림을 보여 주고 있다.

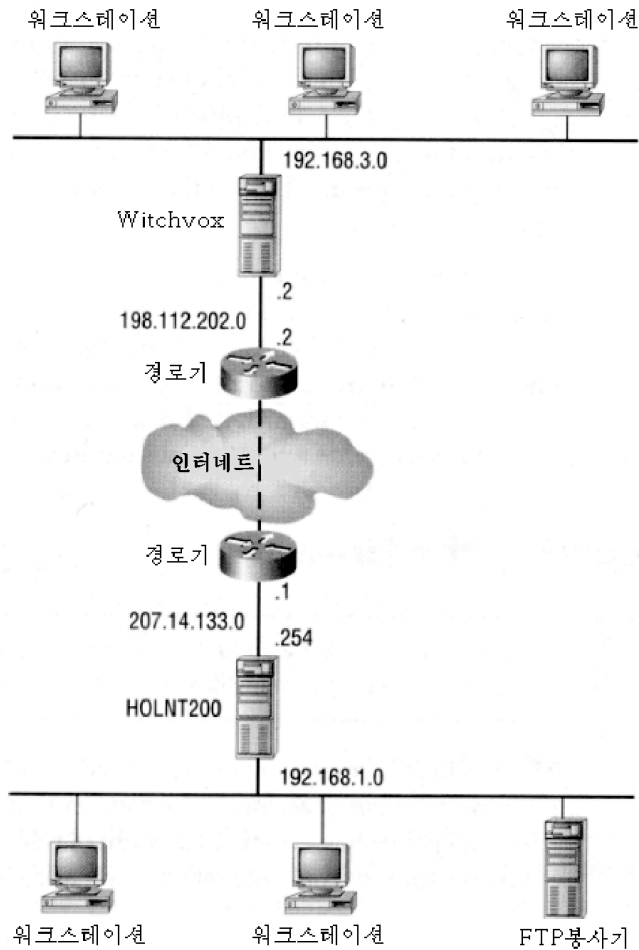



그림 10-4. VPN의 실례

그림은 두개의 원격망싸이트를 보여 준다. 하나는 HOLNT200이라고 하는 방화벽의 뒤에 있고 다른 하나는 Witchvox라고 하는 방화벽의 뒤에 있다. HOLNT200의 뒤에는 재정정보와 관련한 파일들을 가지고 있는 하나의 FTP봉사기가 있다. 목표는 안전한 통로를 설치하여 Witchvox의 다른쪽에 있는 의뢰기들이 안전한 방법으로 재정파일들을 검색할수 있게 하는것이다. FTP는 모든 자료를 평문으로 보내기때문에 이 재정정보들이 손상되지 않도록 담보하기 위하여 VPN을 리용하려고 한다.

VPN통로의 매끝에 대하여 암호화령역을 정의하여 VPN을 구성한다. 이것은 방화벽이 암호화된 자료흐름을 어느 원격망과 교환하는가를 확인하게 한다. 실례로 192.168.1.0망으로 향하는 자료흐름들을 암호화하도록 방화벽Witchvox를 구성할수 있다. 또한 Witchvox가 192.168.1.0망에서 받은 모든 자료흐름을 복호화하도록 지시할수 있다. HOLNT200은 같은 방법으로 구성되는데 원격암호화령역은 192.168.3.0으로 정의된다.

필요한 망객체들의 구성

첫 단계는 요구되는 모든 망객체들을 만드는것이다. 매개 방화벽은 다음의 대상들을 가져야 한다.

- 국부암호화령역을 위한 하나의 망객체 또는 집단
- 원격암호화령역을 위한 하나의 망객체 또는 집단
- 자기자신을 위한 워크스테이션대상
- 원격방화벽을 위한 워크스테이션대상

망객체들의 정의

국부망객체를 정의하지 않았다면 아래와 같이 하나의 대상을 정의하여야 한다.

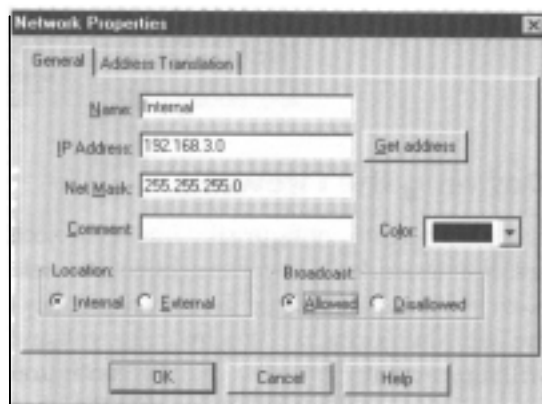



그림 10-5. Network Properties화면

이것은 Secutity Policy칸의 기본차림표에서 Manager → Network Objects → New → Network를 선택하여 실행될수 있다. 이렇게 하면 그림 10-5의 Network Properties화면이 나온다. 이 대상에 이름을 주고 적당한 부분망주소와 마스크를 할당한다. 이 구성은 Witchvox우에서 수행되며 따라서 192.168.3.0망객체의 위치는 내부인것으로 식별된다. OK를 눌러 이 항목을 보관한다.

만일 망토막이 여러개라면 매개에 대하여 정의한다. 모든 망객체들을 정의하였다면 집단대상을 창조하여 이 매 망객체들을 그안에 넣어야 한다. 다음에 암호화령역을 정의하여야 한다. 령역을 식별할 때 하나의 대상만을 지정하여야 한다. 만일 여러개의 망토막들을 식별하여야 한다면 망객체들의 집단을 규정하여 이것을 할수 있다.

내부부분망들을 식별하였다면 원격암호화령역에서의 부분망들도 식별하여야 한다. 이것은 국부토막에서와 같이 추가적인 망객체를 창조하여 실현한다. 차이점은 대상의 위치가 그림 10-6에서 보는바와 같이 External로 되여야 한다는것이다. 그림 10-6에서 Witchvox방화벽을 구성하는데 192.168.1.0대상은 원격망의 부분으로 된다. 그러므로 그것은 방화벽의 밖에 있는것으로 식별된다.

일러두기

국부대상들과 혼돈하지 않기 위하여 원격부분망들에 색갈을 할당할수 있다.

그림 10-6. 원격부분망들은 External로 정의되여야 한다

방화벽들의 정의

이제는 방화벽대상들을 구성하여야 한다. Security Policy칸의 기본차림표로부터 Manager → Network Objects → New → Workstation을 선택하여 그 방화벽에 대한 망객체를 구성한다. 그림 10-7에서는 Witchvox방화벽을 구성하고 자기자신을 표현하는 워크스테이션대상을 만든다. 이 구성에서는 방화벽의 외부NIC로부터 IP주소를 리용하며 그 위치는 내부인것으로 정의한다.

다음은 Encryption칸을 찰칵하고 국부암호화령역을 정의하고 암호화방법을 선택한다. 이것을 그림 10-8에 보여 준다. Encryption Domain에서 Other가 선택되며 국부망객체가

지정된다. 그리고 Encryption Schemes Defined에서 SKIP가 선택되였다.

그림 10-7. Witchvox방화벽대상에 대한 General표쪽

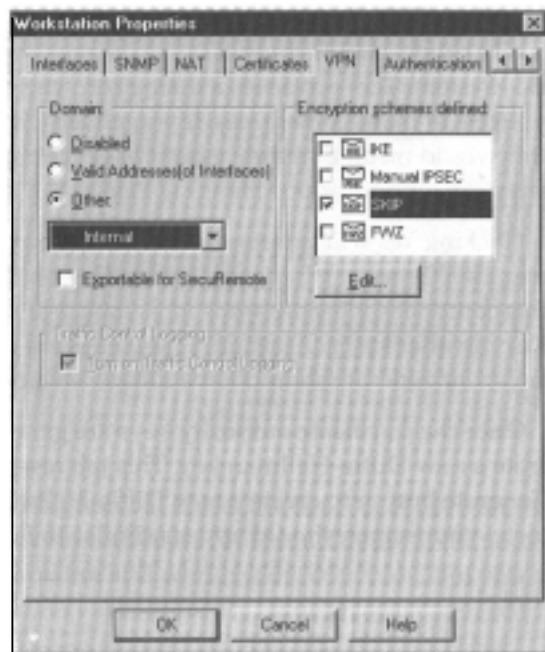



그림 10-8. Witchvox방화벽대상에 대한 Encryption표쪽

SKIP암호화를 선택하였으면 Edit단추를 찰칵한다.

그러면 그림 10-9에 보여 준 SKIP Properties창문이 나온다. 이 칸에는 등록된 열쇠정보가 없다. 원격체계들을 인증하기 위하여서는 증명서열쇠를 생성하여야 한다. 이 구성에서 Local이 증명서권한으로 지정된다. 다른 체계를 지적하려면 Remote를 선택하고 증명서권한을 위한 미리 정의된 대상을 선택하여야 한다.

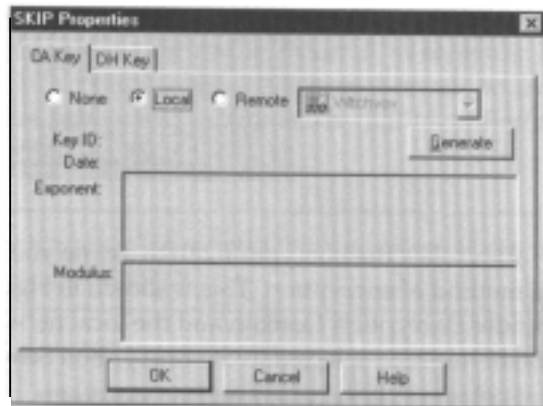



그림 10-9. SKIP Properties 의 CA열쇠표쪽

이 체계에 대한 새로운 증명서권한열쇠(CA열쇠)를 창조하려면 Generate단추를 찰칵한다. 그러면 SKIP관리열쇠를 변경하는것에 대하여 경고하는 대화칸이 나온다. 만일 이미 다른 싸이트들과 VPN련결을 가지고 있다면 이것은 그들이 수동적으로 새 열쇠를 가져 와야 한다는것을 의미한다. 이것이 새로운 구성이므로 열쇠를 변경하는것은 문제가 아니다. Yes를 눌러 계속한다.

Yes를 찰칵하면 새로운 관리열쇠가 생성되고 있다는것을 통지하는 새로운 대화칸이 나온다. 체계의 처리기속도에 따라 몇초 또는 몇분이 걸릴수 있다.

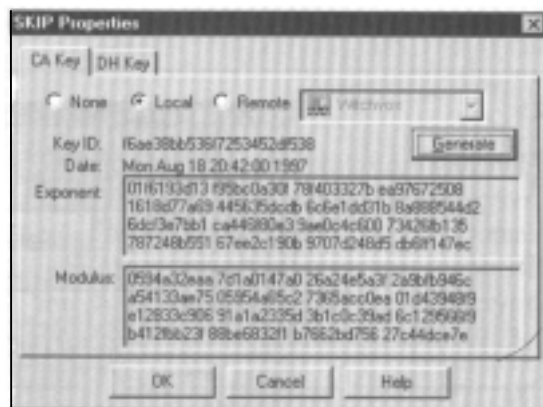



그림 10-10. 열쇠생성이후의 CA Key표쪽

그림 10-10은 열쇠생성후의 CA Key칸을 보여 준다. 이 열쇠들은 이 특정의 체계에서 일의적이다. 생성된 열쇠들은 서로 다른 값들을 가져야 한다.

CA열쇠들이 생성되였으면 DHKey칸을 선택하여 새로운 Diffie-Hellman열쇠를 생성한다. 이 칸은 CA Key칸과 류사하다. Generate단추를 눌러서 새로운 Diffie-Hellman 열쇠를 창조한다. 열쇠생성이 끝나면 그림 10-11과 같은 화면이 나타난다.

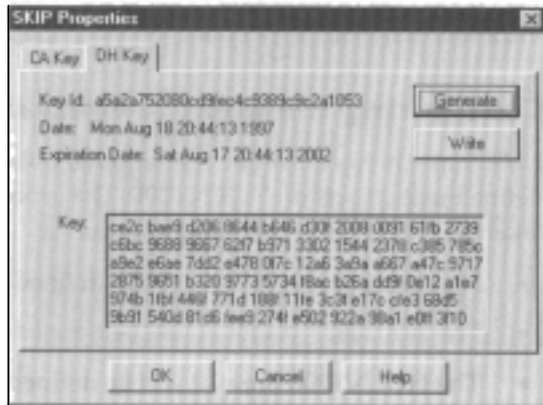



그림 10-11. SKIP Properties에 대한 DH Key표쪽

주 의

CA열쇠들과 마찬가지로 Diffie-Hellman 열쇠는 체계에 일의적이며 따라서 그림에서 보여 준것과 같은 열쇠렬을 얻을수 없을것이다.

마지막으로 Write단추를 눌러서 이 열쇠를 보관하고 OK를 찰각한다.

그림 10-12. 방화벽 HOLNT200에 대한 Genera속성

국부방화벽에 대상을 구성하였으므로 이제는 VPN통로의 다른 끝에 있는 방화벽에 대한 대상을 정의하여야 한다. 이것을 그림 10-12에서 보여 주었다.

아직 Witchvox우에서 동작하고 있지만 방화벽 HOLNT200을 위한 대상을 정의한다. 그 체계는 자기의 외부IP주소와 결합되여 있으며 위치는 External로 정의되여 있다.

General칸의 내용을 다 채우고 OK를 눌러 보관한다.

원격방화벽우의 대상을 정의할 때까지 HOLNT200대상의 Encryption칸에는 아무것도

써넣지 않는다. 이때 Network Objects화면의 Close를 눌러 이 대상들을 방화벽에 설치한다. 이것은 Security Policy칸의 기본차림표에서 Policy → Install을 선택하여 진행한다.

원격방화벽의 구성

Witchvox의 대상들을 정의하였으면 이제는 HOLNT200의 대상들도 정의하여야 한다. 이 과정은 지금까지 한 과정과 같은데 다음의 내용들이 다르다.

- 192.168.1.0부분망은 External이 아니라 Internal로 정의된다.
- 192.168.3.0부분망은 Internal이 아니라 External로 정의된다.
- HOLNT 200방화벽은 External이 아니라 Internal로 정의된다.
- 열쇠들은 HOLNT 200대상에 대하여 생성된다.
- Witchvox는 Internal이 아니라 External로 정의된다.

이 대상들이 만들어 지면 Security Policy칸의 기본차림표로부터 Policy → Install을 선택하여 HOLNT 200에 그것들을 설치한다.

열쇠교환

열쇠들을 교환하기 위하여서는 Witchvox방화벽에 돌아 가서 HOLNT200을 위하여 창조한 대상을 편집한다. HOLNT 200에 대한 Workstation Properties화면이 나오면 Encryption 칸을 선택한다. Encryption Domain에서 192.168.1.0망 (HOLNT 200뒤에 있는 원격망) 에 대하여 만든 대상을 결합한다. 또한 Encryption Schemes Defined에서 SKIP를 선택한다. 그러면 그림 10-13과 같은 대화칸이 나타난다.

그림 10-13. 원격방화벽 HOLNT 200에 대한 Encryption속성

SKIP속성들을 관리하기 위하여 Edit단추를 찰칵하면 Witchvox대상에서와 류사하지만 약간 다른 화면이 나타난다.

이것을 그림 10-14에 보여 준다. 증명서권한이 국부체계로 정의될 대신에 Remote가 선택되며 HOLNT 200대상은 원격체계로 선택된다.

Generate단추는 없고 그대신에 Get단추가 있다.

그 리유는 새로운 열쇠를 생성하는것이 아니라 열쇠를 HOLNT 200에서 가져 오기때문이다.

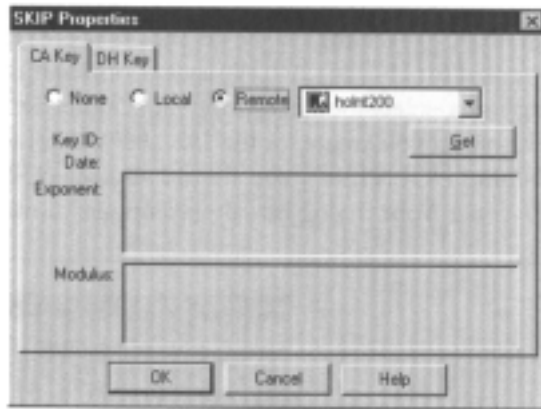



그림 10-14. HOLNT 200의 SKIP속성의 CA Key표쪽

Get단추를 찰칵하면 원격증명서를 검색할수 있다.

그 열쇠들을 보내는것이 HOLNT 200임을 확인하기 위하여 인증없이 열쇠들을 가져간다는것을 경고하는 대화칸이 나온다. 이것은 정상이다. 즉 이것은 두 체계사이의 첫 열쇠교환이며 따라서 원천을 인증하는데 리용될수 있는 이전의 열쇠정보는 없어 지게 된다. 또한 열쇠값을 수동적으로 확인하여야 한다는것을 알린다. 이것은 원격방화벽관리자를 불러서 받은 열쇠값들을 읽는 방법으로 실행할수 있다. 그들은 자기들이 국부방화벽대상에 대하여 생성된 열쇠값들을 비교하여야 한다.

우리의 실례에서는 HOLNT 200방화벽에 가서 HOLNT 200대상을 편집하고 Encryption칸의 SKIP속성들을 검사하는 방법으로 정확한 열쇠들을 받았다는것을 확인할수 있다.

CA Key들을 받았으면 DH Key표쪽을 찰칵하여 Diffie-Hellman열쇠를 가져 온다. CA Key표쪽에서와 같이 Generate단추는 Get단추로 바뀐다. Get단추를 찰칵하여 열쇠를 원격방화벽으로부터 가져 온다. 이때 그림 10-15와 같은 화면이 펼쳐 진다. CA열쇠와 마찬가지로 원격방화벽관리자를 찾아서 열쇠값을 수동적으로 확인하여야 한다. Write단추를 찰칵하면 OK단추를 찰칵하여 우의 조작들을 보관한다.

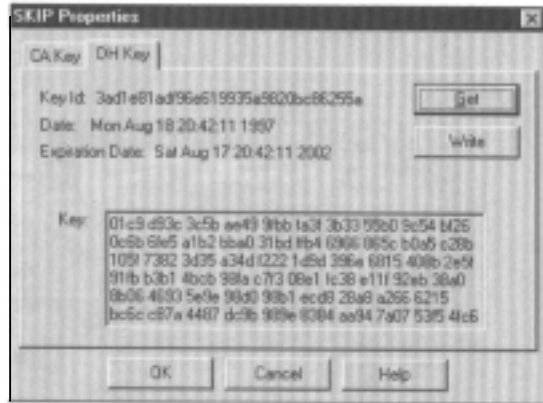



그림 10-15. HOLNT200의 SKIP속성에 대한 DH Key표쪽

원격방화벽에서 열쇠를 가져오기

Witchvox는 지금 HOLNT200으로부터 필요한 모든 열쇠정보들을 가지고 있다. 이제는 HOLNT200방화벽에 가서 Witchvox대상을 편집하여 HOLNT200이 필요한 열쇠정보들을 가져 갈수 있게 하여야 한다. 이 과정은 이미 수행한것과 같은데 다른것은 Witchvox의 Encryption칸에서 정의되는 Encryption Domain이 부분망 192.168.3.0(Witchvox뒤에 있는 부분망)을 지적하여야 한다는것이다. 나머지 단계들은 다 같다. 일단 HOLNT200이 열쇠들을 가져 왔다면 그것들을 수동적으로 확인하여야 한다.

보안방책의 변경

요구되는 모든 망객체들을 창조하고 열쇠들을 교환하였다. 이제는 규칙들의 모임을 정의하여 방화벽이 언제 VPN을 리용할것인가를 알게 하여야 한다. 이것은 PolicyEditor의 쪽대기에서 하나의 새로운 규칙을 만들고 국부 및 원격망을 Source 및 Destination렬에 추가함으로써 수행된다. Service렬에서는 기정으로 Any(이것은 두 암호화령역사이의 모든 자료흐름을 암호화한다.)를 선택하거나 어떤 특정의 봉사만을 암호화하도록 선택할수 있다.

Action렬에서 오른쪽찰칵하여 Encrypt를 선택한다. 규칙들은 그림 10-16의 1행과 같다.

주 의

국부 및 원격암호화령역들은 Source 및 Destination행들에 나타나야 한다.

이제는 이 특정의 VPN에 대한 암호화속성들을 정의하여야 한다. 이것은 다시 Action칸에서 오른쪽찰칵하여 수행되는데 이때 Edit Properies를 선택하여야 한다. 이때 그림 10-17과 같은 Encrytion Properties창문이 나온다. 방화벽-1이 여러가지 형태의 암호화를 지원하기때문에 여러개의 VPN들우에서 여러가지 형태로 암호화를 리용할수 있다. 그러므로 이 VPN통로에 리용하려는 암호화형태를 지정하여야 한다.

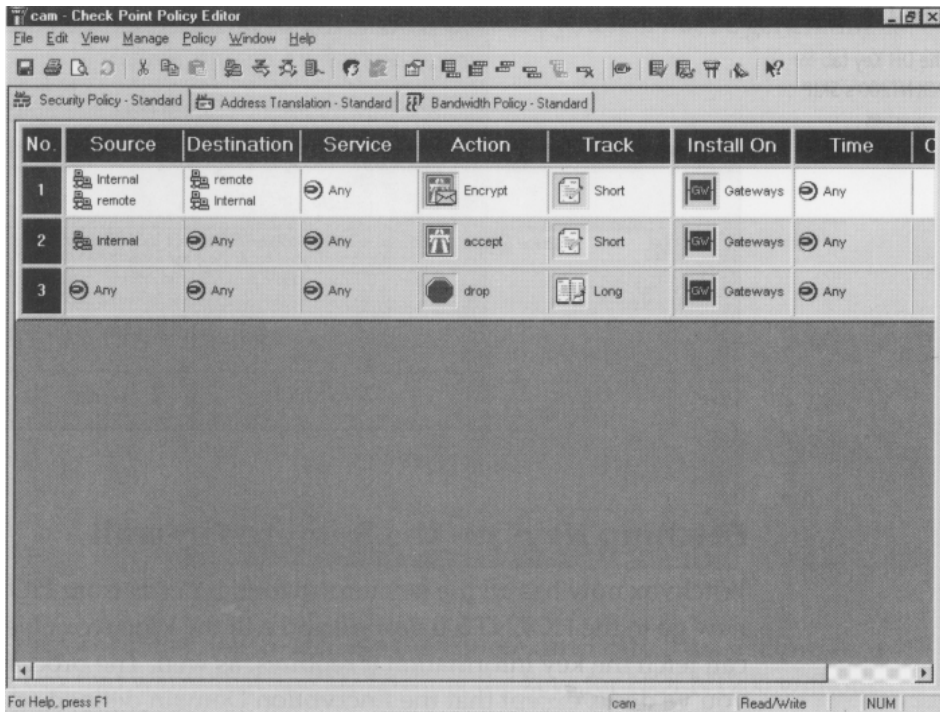



그림 10-16. 어느 자료흐름이 암호화되여야 하는가에 대한 규칙의 정의

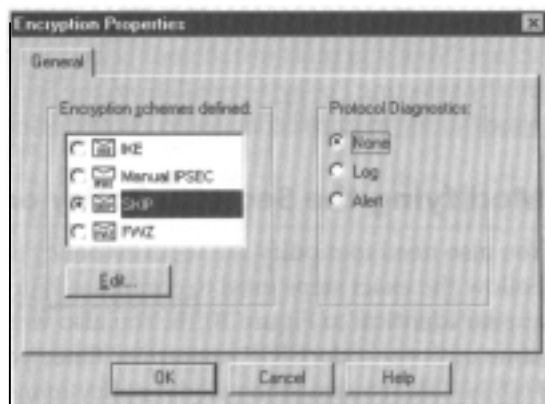



그림 10-17. Encryption Properties창문

Encryption Properies창문에서 SKIP를 선택하여 Edit단추를 찰칵한다. 그러면 그림 10-18과 같은 SKIP Properties창문이 나온다. 다음과 같은 항목들을 선택할수 있다.

Kij Algorithm 이것은 체계들이 Crypt와 MAC열쇠들을 교환할 때 리용하는 암호화방법을 설정한다.

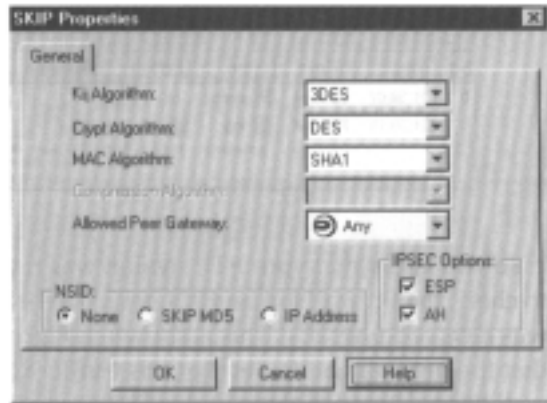



그림 10-18. SKIP Properties창문

Crypt Algorithm 이것은 자료를 암호화하고 복호화할 때 리용하는 암호화방법을 설정한다.

MAC Algorithm VPN통로의 원격끝에서 체계를 인증할 때 리용하는 암호화방법을 설정한다.

Allowed Peer Gateway 이것은 누가 VPN전송을 시작하겠는가를 정의한다. 만일 Any가 선택되면 매 암호화령역과 결합된 방화벽이 암호화자료를 전송하게 된다. 만일 특정의 체계가 지적되면 Security Policy Editor에서 2개의 규칙이 또 요구된다.

NSID 이것은 이름공간 ID들을 선택한다. None을 설정하면 교갑화된 머리부에 있는 NSID정보를 포함한다.

IPSEC Options SKIP가 IPSEC와 함께 리용되면 이 항목들중 하나 또는 2개가 설정되여야 한다. ESP항목은 암호화를 설정하며 AH항목은 인증을 설정한다.

이 특정의 VPN련결을 위한 SKIP항목들을 설정한 다음에는 OK를 두번 찰칵하여 보관한다.

그러면 Security Policy 기본화면으로 돌아 간다.

이제는 방책변화들을 설치하여 그것이 동작하게 하여야 한다. 그러기 위하여 Security Policy칸의 기본차림표에서

Policy → Install을 선택한다.

이상으로 VPN련결을 설치하기 위한 Witchvox에로의 모든 요구되는 변화가 완성된다.

원격방화벽에서의 보안방책의 수정

이제는 HOLNT200에서의 보안방책과 SKIP속성들을 수정해야 한다. 이것은 Witchvox를 구성할 때와 같다. 그 규칙들은 그림 10-16에서와 꼭 같다. 또한 SKIP속성들에서 같은 항목들을 선택하였는가를 확인하여야 한다. HOLNT200우의 모든 방책변경이 끝나면 그것을 설치하여 변화가 동작하게 해야 한다.

VPN검사

우에서와 같이 하여 VPN의 설치가 완료되였다. 이제 남은것은 VPN을 시험하여 그것이 정확히 기능하는가를 확인하는것이다. 그러기 위하여 Witchvox뒤의 192.168.3.0 망으로부터 HOLNT200뒤에 있는 FTP봉사기에로 하나의 FTP대화를 기동한다.

No	Time	Origin	Type	Action	Service	Source	Destination	Proto.	Rule
0	21:39:07	Firewall	control	ctl					
1	21:39:15	Firewall	log	encrypt	ftp	192.168.3.10	192.168.1.10	tcp	1

그림 10-19. Witchvox의 FTP 기록파일항목

만일 Witchvox우의 방화벽경과기록파일을 보면 그림 10-19와 같은 나가는 대화를 볼수 있다. 첫째 기록항목은 192.168.3.10에서 나와서 원격 FTP봉사기의 IP주소인 192.168.1.10으로 가는 FTP대화를 보여 준다. 여기서 자료흐름이 암호화되였다는것을 알수 있다.

이제는 FTP대화가 성과적으로 전송되였다는것을 알수 있다. 또한 전송이 정확히 수신되였다는것을 확인하기 위하여 HOLNT200우의 방화벽경과기록파일을 검사하여야 한다. 이것을 그림 10-20에 보여 준다. 여기서 기록파일은 방화벽이 이 자료흐름을 복호화하여야 한다는것을 지적한다. 방화벽은 FTP봉사기의 진짜이름(LAB31)을 알고 있기때문에 목적지IP주소로 이 이름을 바꾸어 넣었다는것을 알수 있다.

fw.log - FireWall-1 Log Viewer
File Edit View Select Window Help
Log

No	Time	Origin	Type	Action	Service	Source	Destination	Proto.	Rule
0	21:32:38	holnt200	control	ctl					
1	21:32:48	holnt200	log	decrypt	ftp	192.168.3.10	LAB31	tcp	1

그림 10-20. HOLNT200의 FTP기록파일항목

자료흐름의 확인

이 모든것이 정확하지만 진짜 시험은 망분석기를 통하여 방화벽에 의해 전송되는 자료흐름을 해신하는것이다. 경과기록의 항목들은 자료흐름이 암호화되고 복호화될것을 요구하지만 절대로 검사에 지장이 되지는 않는다.

망분석기는 전송되는 파케트의 내용들을 보여 줄것이다.

만일 자료흐름안에 있는 재정정보 같은것을 읽을수 있다면 그때는 문제이다.

```
LANalyzer for Windows
File  Monitor  Alarms  Capture  Decode  Window  Help
D:\VPNIMA~1\DECRYPT.TR1
No. Source        Destination   Layer Summary                              Error Size Interpacket Time Absolute Time
  7 00805F48454B  006097D82737  tcp   Port:FTP-DATA --> 1047 ACK                     64          316 µs 9:47:12 PM
  8 00805F48454B  006097D82737  tcp   Port:FTP-DATA --> 1047 ACK PUSH               292            2 ms 9:47:12 PM
  9 006097D82737  00805F48454B  tcp   Port:1047 --> FTP-DATA ACK                     64          177 ms 9:47:12 PM

        Station:192.168.1.10 ---->192.168.3.10
        Protocol: TCP
        Version: 4
        Header Length (32 bit words): 5
        Precedence: Routine
              Normal Delay, Normal Throughput, Normal Reliability
        Total length: 274
        Identification: 10245
        Fragmentation not allowed, Last fragment
        Fragment Offset: 0

   0: 00 60 97 D8 27 37 00 80 5F 48 45 4B 08 00 45 00 |.`..'7.._HEK..E.
  10: 01 12 28 05 40 00 80 06 4C 7C C0 A8 01 0A C0 A8 |..(.@...L|......
  20: 03 0A 00 14 04 17 00 D3 4A A9 00 6D 77 58 50 18 |........J..mwXP.
  30: 22 38 42 40 00 00 53 6D 69 74 68 2C 20 4A 69 6D |"8B@..Smith, Jim
  40: 20 20 20 20 20 20 34 34 32 38 20 33 33 36 39 20 |      4428 3369
  50: 32 37 30 30 20 32 38 34 33 20 20 20 20 20 39 2F |2700 2843     9/
  60: 39 39 20 20 20 20 24 32 30 30 2E 31 35 0D 0A 6A |99    $200.15..j
  70: 6F 6E 65 73 2C 20 57 6F 6C 6C 79 20 20 20 20 34 |ones, Wolly    4
  80: 31 31 31 20 33 37 38 39 20 31 35 30 30 20 32 38 |111 3789 1500 28
  90: 33 32 20 20 20 20 20 36 2F 39 39 20 20 20 20 24 |32     6/99    $
  A0: 31 30 37 2E 35 33 0D 0A 41 70 70 6C 65 2C 20 41 |107.53..Apple, A
  B0: 6D 62 65 72 20 20 20 20 34 37 31 37 20 38 36 34 |mber    4717 864
  C0: 33 20 31 32 33 34 20 38 37 33 33 20 20 20 20 20 |3 1234 8733
  D0: 37 2F 39 39 20 20 20 20 24 32 2C 32 33 32 2C 34 |7/99    $2,232,4
  E0: 35 0D 0A 4E 6F 72 74 68 2C 20 42 61 62 79 6C 6E |5..North, Babyln
  F0: 6F 72 20 34 36 35 32 20 38 34 37 36 20 39 33 38 |or 4652 8476 938
 100: 34 20 32 32 31 39 20 20 20 20 20 32 2F 39 39 20 |4 2219     2/99
 110: 20 20 20 24 31 2C 33 38 39 2C 31 34 0D 0A 0D 0A |   $1,389,14....
```

그림 10-21. 암호화되기전의 자료흐름

그림 10-22. 암호화된후의 자료흐름

그림 10−21은 방화벽에 의해 암호화되기전의 FTP대화의 파케트해신을 보여 준다. 여기서 이것이 명백히 FTP대화임을 구별할수 있다.

또한 이러한 대화를 수행하는 체계들의 IP주소들을 구별할수 있다. 아래의 창문의 정보를 보면 전송되는 자료가 신용카드정보로 나타난다는것을 알수 있다.

그림 10−22는 같은 자료흐름이지만 방화벽의 바깥으로부터의 자료흐름을 보여 준다. 공격자는 누가 VPN을 통하여 전송되는 자료를 얻으려 하는가를 알수 있다. 매 파케트의 전송층규약은 57로 식별된다. 이것은 전송층규약을 통로규약으로 식별하며 교갑화된 파케트에서 리용되는 진짜 전송층내용이나(이 경우에 TCP) 전송층을 통하여 진행되는 봉사를(이 경우에 FTP) 볼수 없게 한다.

가운데창문을 들여다 보면 원천 및 목적지IP주소가 각각 HOLNT200 및 Witchvox의 주소라는것을 알수 있다. 그 자료흐름의 진짜원천 및 목적지주소는 보이지 않는다. 이것은 암호화된 파케트안에 전송층과 봉사를 숨기는것과 결합하여 공격자가 그 자료전송이 더 가치 있는지를 알수 없게 한다. 사실 이 모든 수집된 자료흐름이 하나의 대화로부터 나왔다는것을 검증할 방법이 없다. 우의 창문에 렬거된 매 파케트들은 동시에 진행되는 여러 통신대화들로부터 올수 있다.

FTP대화를 찾기 위하여 공격자는 수많은 파케트들을 복호화하여야 한다.

진짜시험은 아래의 창문이다. 자료는 지금 암호문으로 되여 더이상 읽을수 없다. 그러므로 공격자는 그림 10−21에서와 같이 포장된 자료를 읽을수 없게 된다. 이 정보를 얻기 위하여서는 공격자는 어느 정보가 재정정보인가를 알아서 그것을 전체조사공격으로 복호화하여야 한다.

이 두개의 파케트경로가 주어 지면 VPN이 정확히 기능하고 있으며 두 암호화령역사이를 흐르는 자료가 암호화되고 있다는것을 알수 있다.

요 약

이 장에서는 가상사설망의 의미를 정의하고 언제 VPN을 리용하는것이 좋은가에 대하여 보았다. 또한 어떤 VPN제품들이 있으며 어떤 종류가 좋은가에 대하여 보았다. 마지막으로 두개의 방화벽사이에서의 VPN의 구성을 보고 자료흐름을 통과시킬 때의 그 효과에 대하여 보았다.

다음장에서는 비루스에 대하여 보고 망에서 어떻게 이 파괴적인 코드들을 없앨수 있는가에 대하여 고찰한다.

제１１장. 비루스, 트로이목마, 웜

모든 체계관리자들은 반드시 비루스에 대하여 관심을 돌려야 한다. 이 크지 않은 코드토막이 체계에 막대한 손실을 줄수 있으므로 매우 심중한 문제로 고려된다. 많은 기관들이 이 문제로 하여 생산력과 지적능력에서 큰 손실을 보고 있다. 명백히 비루스의 공격을 받고 그것을 회복하는것은 비루스를 사전에 막아 내는것보다 훨씬 더 많은 비용이 든다.

비루스 : 통계자료

1990년대 초에는 상대적으로 비루스의 영향을 적게 받았다. 그러나 인터네트의 도입과 함께 콤퓨터체계들이 비루스의 피해를 받을 위험은 증가되였다. 1997년에 NCSA(National Center for Supercomputing Applications)의 한 조사연구는 전체 회사들중 99.33%가 최근에 비루스의 피해를 받은적이 있다는것을 보여 주었다.

1996년에 매달 비루스감염률은 콤퓨터 1000대중 10대이상이였으며 1997년에 그것이 3배이상으로 증가되였다. 2000년 10월에 제출한 ICSA(지금은 TruSecure)의 연구에 의하면 최근 5년동안 콤퓨터 1000대당 비루스감염률이 매해 적어도 두배씩 증가하여 2000년에는 1000대당 160대로 늘어 났다는것을 보여 주었다.

또한 다음과 같은 연구자료들도 있다.

- 모든 회사들은 매해 비루스로 인하여 막대한 피해를 보고 있다.
- 조사된 회사들중 40%이상이 비루스감염으로 자료를 류실 당한적이 있다.
- 회사들중 3분의 2가 비루스의 침습에 의하여 전자우편들을 손실 당한적이 있다.
- 조사한 회사들중 하나만이 년중에 비루스의 피해를 한번도 입지 않았는데 이것은 감염률이 99.67%임을 보여 준다.
- 주요 비루스피해(한번에 25대이상에 피해를 주는)는 51%의 회사들에서 나타났다.
- 그중 80%는 전자우편접촉을 통하여 비루스가 전파되였다.
- 봉사기들중 64%가 한시간이상 계속된 비루스감염으로 하여 평균 21시간동안 작업을 하지 못하였다.
- PC들중 70%만이 완전시간 자동반비루스체계에 의해서 보호되였다.
- 조사에 응한 회사나 기관의 76%가 비루스문제가 전해(1999년)에 비하여 더 심각해 졌다고 하였다.

조사결과는 또한 기동비루스나 플로피디스크비루스는 거의 나타나지 않는다는것을 보여 주었다. 이것은 주로 공유하는 플로피디스크들에서 비루스들이 전파된다고 한 1997년 NCSA조사와는 상반되는것이다. 지금은 주로 전자우편을 통한 파일공유로 하여 인터네트가 플로피디스크를 대신하여 파괴적인 코드들을 전파시키고 있다.

주 의

비루스는 콤퓨터에만 있는것이 아니다. 2000년 8월에 처음으로 PDA (Personal Digital Assistants)들에 영향을 준 파괴적인 코드가 기록되였다. Liberty Crack 라고 하는 프로그람은 현실적으로 Palm OS가 동작하는 휴대용 장치로부터 응용프로그람들을 쓸어 버렸다.

같은해 6월에는 콤퓨터에서 동작하는 Timofonica 비루스가 나타났는데 그것은 어떤 본문통보문을 에스빠냐의 모든 휴대용전화기들에 전송하도록 설계되였다.

비루스란 무엇인가

비루스에 대한 정확한 정의는 오래동안 론의되였다. 전문가들은 진짜비루스를 특징지으며 그것을 다른 형태의 프로그람들과 구별하게 하는 본질적인 정의에 대하여 여러해동안 론쟁하였다. 사람들은 보통 비루스, 웜, 트로이목마 등을 《비루스》라는 하나의 이름으로 불러 왔다. 이러한 형태의 모든 프로그람들을 포괄적으로 특징 짓는 정의가 없는것으로 하여 이 정의는 정확하다고 볼수 없다.

일반적으로 비루스는 다음의 3가지 기능을 가진 프로그람이다.

- 복제
- 잠복
- 폭탄

이 3가지 속성이 합쳐 져서 비루스프로그람을 형성한다.

복제

비루스는 반드시 어떤 복제방법 즉 자기자체를 재생하거나 복제하는 기능을 가져야한다. 비루스가 다른 파일에 자기자체를 복제하면 이것을 때로 감염이라고 한다. 사람들은 대부분 비루스를 자기체계에 모르고 태우기때문에 비루스가 전파되게 된다.

복제는 비루스가 기억기에 들어 가서 CPU동작에 접근할 때 일어 난다.

비루스는 하드디스크안에서는 복제되지 않는다. 이것은 감염된 파일이 실행될 때에야 비루스가 활동상태로 된다는것을 의미한다. 《실행된다》는것은 일반적인 의미이다. 이것은 감염된 실행파일의 기동 또는 감염된 Microsoft Word문서가 본문편집기에 적재되는것 등을 의미한다.이때 이것들은 CPU에 의하여 처리되며 이를 통하여 비루스코드를 전파시킬수 있다.

파일감염

복제방법에는 두가지가 있다. 그중 하나는 파일감염이다.

이 복제방법은 자기자체를 다른 파일에 붙이는 비루스의 능력에 기초하고 있다. 리

론적으로 임의의 형태의 파일도 공격 받을수 있다. 그러나 공격자들은 CPU순환에 접근할수가 있는 파일에 주목한다. 이것은 직접 실행을 통하여 또는 응용프로그람에 의해 처리된 코드에 의하여 진행된다.

실례로 Word 문서는 기억기상에서 임의의 형태의 지령으로도 직접 실행되지 않는다. Microsoft Word를 실행하면 Word문서에 매몰된 마크로지령들을 읽을수 있으며 기억기에서 그것을 실행할수 있다. 따라서 Word 문서가 감염되면 Word응용프로그람은 복제를 일으킨다.

오래전부터 이러한 형태의 비루스들은 DOS의 ANSI.SYS구동기를 침습하였다. 임의의 본문문서는 매몰된 ANSI지령들을 포함한다. ANSI구동기가 태워 져 있다면 사용자가 파일의 본문을 보기만 해도 이 지령이 파일로부터 분석되여 실행된다. 새로운 원천코드파일에 자기를 매몰하는 비루스들도 있다. 코드가 콤파일되면 비루스는 CPU에 접근하여 복제된다.

그러나 대부분의 감염은 실행파일을 감염시키는것이다. PC에서 이런 파일은 확장자가 com, exe, pe 또는 bat이다. 비루스는 파일의 시작부분에 작은 코드쪼각을 첨가한다. 이것은 파일이 실행될 때에 비루스가 기억기에 있다는것을 보여 준다. 그리고 비루스는 나머지코드들을 파일의 내부 또는 끝에 넣는다.

일단 파일이 감염되면 두가지 형태의 복제가 진행될수 있다. 이 두 가지를 상주복제와 비상주복제라고 한다. 상주복제비루스는 기억기에 들어 가서 다른 프로그람이 실행되기를 기다렸다가 실행되면 감염시킨다. Cabanas와 같은 비루스들은 지어 Windows NT와 같은 보안된 기억체계들우에서도 감염을 일으킨다. 비상주복제비루스는 디스크우의 하나 또는 그이상의 실행파일들을 선택하고 기억기안에서 실행될 때를 기다리지 않고 직접 감염시킨다. 이것은 감염된 실행파일을 실행시킬 때마다 일어 난다.

때때로 비루스는 존재하는 파일을 감염시키지 않고 비루스코드의 복제를 함께 하기 위하여 조작체계의 확장자 검색순서를 리용할수 있다. 이런 형태의 비루스를 동료(companion)비루스라고 한다. 동료비루스는 합법적인(정당한) 실행파일이 실행되기전에 자기의 실행파일이 실행되게 한다.

실례로 실행파일 gl.exe로 초기화한 계산프로그람을 가지고 있다고 하자. 계산프로그람을 gl만 건반으로 쳐서 실행시킨다면 공격자는 기억기에 적재된 gl.com이라는 비루스를 생성하여 gl.exe파일의 조종을 빼앗을수 있다. 이것은 파일확장자가 정의되지 않았으면 DOS와 Windows가 먼저 com파일을 실행하고 그다음 exe, bat파일의 순서로 실행하기때문이다. 만일 이런 파일이 있으면 조작체계는 검색하기를 그만두고 프로그람을 실행한다.

우의 실례에서 조작체계는 진짜파일(확장자 exe)을 찾기전에 비루스파일(확장자 com)을 찾아서 그 파일을 실행한다.

기동분구복제

복제의 두번째 형태는 기동분구복제이다. 이러한 비루스는 디스크가 처음 호출될 때 또는 기동될 때 읽게 되는 디스크의 구역을 감염시킨다. 이것은 1차기동레코드나 조작체계의 기동분구 등이 될수 있다.

주　　의

파일과 기동분구의 복제기능을 다같이 가진 비루스를 다원비루스라고 한다.

이러한 구역을 감염시키는 비루스는 체계명령들을 가지고 그것들을 디스크의 다른 구역으로 움직여 놓는다. 그다음 비루스는 자기의 코드를 기동기록호에 마음대로 가져다 놓는다. 체계가 초기화되면 비루스는 기억기에 적재되여 체계지령을 위한 새로운 위치(주소)만을 가리킨다. 이것은 비루스가 기억에 현재 상주하고 있다는것을 제외하고는 체계가 정상으로 기동하게 한다.

주　　의

기동분구비루스는 복제를 위하여 감염된 디스크에서의 프로그람실행을 요구하지 않는다. 디스크를 호출하기만 해도 충분하다. 실례로 대부분의 PC들은 플로피디스크구동기의 조작을 검사하는 체계검사를 진행한다. 이러한 검사과정에 플로피디스크에 있던 기동분구비루스가 동작하게 된다. 이렇게 되면 하드구동기도 감염된다.

기동분구비루스가 복제되자면 디스크와 디스크의 접촉이 필요하다. 두개의 디스크들이 같은 기계에 소속되여야 한다. 실례로 다른 체계에서 기동분구비루스가 들어 있는 체계우의 공유된 등록부에 접근하면 비루스는 그 체계에 복제될수 없다.

이것은 두개의 기계가 기억기나 처리소자를 공유하지 않기때문이다.

그런데 기동분구비루스를 전파시킬수 있는 dropper라는 프로그람은 망까지 건너 간다. dropper는 비루스를 효과적으로 설치한다. dropper는 자기자체에 비루스를 감추고 반비루스쏘프트웨어를 속여 넘긴다. 또한 사용자들이 프로그람을 실행하도록 재촉하기 위하여 쓸모 있는 프로그람들을 내장하고 있다.

dropper프로그람이 실행되면 비루스가 국부체계에 설치된다.

주　　의

dropper를 리용하여 공격자는 망을 통하여 기동분구비루스를 감염시킬수 있다. 비루스가 일단 들어 간 다음에 비루스를 더 복제하려면 디스크-디스크접근이 요구된다.

파일감염과 기동분구복제의 공통적인 특성

파일과 기동분구비루스복제에서 공통적인것은 비루스가 자기를 검출하는 어떤 방법을 가져야 한다는것이다. 이것은 감염의 반복으로 일어 나는 혼란을 막기 위하여서이다. 만일 혼란이 일어 나면 프로그람은 쓸모 없게 되거나 사용자가 어디엔가 틀렸다는것을 알수 있게 된다.

만일 복제를 계속할수 없으면 비루스는 사멸하고 만다.

재미 있는 Catch-22

비루스제작자들이 복제를 막기 위하여 쓰는 한가지 방법은 비루스를 검사하고 파일의 감염을 막는데도 쓰인다. 많은 비루스제작자들은 자기가 알고 있는 특별한 코드렬로 자기의 비루스를 알아 본다. 그러면 비루스는 파일을 감염시키기전에 이 코드렬을 찾도록 설계된다. 그런 렬이 있으면 파일은 감염되지 않는다.

반비루스쏘프트웨어는 이 서명코드렬을 찾도록 설계될수 있다. 이것은 쏘프트웨어가 비루스의 존재를 빨리 알수 있게 한다. 또한 정확한 비루스코드가 없이도 이 코드렬을 파일에 붙이면 비루스에 감염되지 않는다.

마크로비루스

마크로비루스는 조작체계와는 반대로 응용프로그람에 의하여 실행되며 따라서 조작체계독립이다.

VBA(Visual Basic for Applications)에 의하여 만들어 지고 Microsoft의 Office(Word, Excel, Access)에 의하여 실행되며 문서에 숨어서 다른 비슷한 문서들에 의하여 류포되며 때때로 체계의 다른 파일들을 감염, 파괴시킨다.

ICSA의 통보에 의하면 마크로비루스는 알려 진 전체 비루스의 80%에 달하며 그 수는 점점 늘어 나고 있다. 마크로비루스의 위험성은 문서의 열기, 보관, 편집 등 응용프로그람리용의 임의의 단계에서 파일을 감염시키는 능력이다. 또한 VBA가 배우기 쉽고 마크로비루스를 약간의 기술로도 능히 만들수 있는것과도 관련된다.

잠 복

복제를 추진시키려면 비루스가 자기의 존재를 감추는 여러가지 기능을 가지고 있어야 한다. 비루스의 동작이 Windows 98과제띠에 나타나면 그것을 제꺽 알수 있다. 비루스들은 자기의 존재를 감추기 위하여 여러가지 교묘한 수법들을 많이 쓴다.

작은 흔적

비루스는 크기가 매우 작아 지는 방향으로 발전하고 있다. 큰 비루스라고 해도 크기가 2KB보다 작을수 있다. 이러한 작은 흔적은 비루스가 작은 기억공간에서 실행될 때 자기를 쉽게 감추게 한다. 비루스를 될수록 작게 하기 위하여 아쎔블러어로 작성한다.

비루스가 작으면 다른 파일에 가붙어도 전체적인 파일크기에 영향을 주지 않는다. 구멍비루스라는것도 있는데 이것은 파일안에서 반복되는 렬(보통 령값)을 찾아서 이 구역을 자기의 구역으로 한다. 이것은 비루스가 파일크기에 영향을 주지 않고 자기의 코드를 삽입하게 한다.

속성위조

파일을 비루스감염으로부터 막기 위하여 초기에 DOS콤퓨터사용자들은 자기의 실행

파일을 읽기전용으로 하였다.

그것은 만일 파일이 위조될수 없으면 비루스에 감염되지 않을것이라고 생각하였기때문이다. 물론 비루스제작자들은 비루스를 감염시키기전에 파일의 속성을 검사하는 코드를 비루스에 추가한다. 만일 속성이 읽기전용으로 되여 있으면 비루스는 읽기전용속성을 변화시켜 파일을 감염시키고 다시 속성을 원래대로 만들어 놓는다. 물론 이 방법은 현대적인 비루스를 막기에는 너무도 약하다.

그러나 다중사용자환경에서 허가준위가 사용자-사용자준위에서 설정되면 사정은 달라 진다. 만일 관리자준위특권이 파일속성을 변화시키게 되여 있다면 비루스는 합법적인 사용자준위에서 진행되는 이 속성을 변화시킬수 없다.

실례로 NetWare봉사기환경에서 합법적인 사용자들이 공유된 등록부에 읽기권한으로 접근한다고 하자. 만일 사용자콤퓨터가 비루스에 감염된다면 비루스는 공유등록부의 파일을 감염시키거나 다른 기계들에 전파할수 없다. 왜냐하면 비루스가 이 파일들을 수정할수 없기때문이다. 물론 관리자의 콤퓨터가 감염되면 사정은 달라 진다. 그러나 역시 최저준위의 권한을 설정하면 안전성도 높이고 비루스의 전파도 막을수 있다.

주 의

흥미 있는것은 구좌보안의 결함이 바로 DOS나 Windows 9x, Mac환경에서 비루스들이 잘 번식되는 리유로 된다는것이다. UNIX나 Windows NT/2000용으로 작성된 비루스들은 매우 적다. 왜냐하면 파일의 속성을 설정하는 능력이 비루스의 복제 및 감염능력을 제한하기때문이다. 이것은 비루스작성자들이 다른 플래트홈들에 주의를 돌리는 요인의 하나이다.

파일속성과 함께 비루스는 또한 파일과 관련된 자료와 시간표를 수정할수 있다. 이것은 파일이 수정되였다는것을 사용자가 알아 채지 못하게 하기 위하여서이다. 비루스가 있는가 보자면 먼저 자료변화를 찾아 보아야 한다. 대부분의 현대적인 비루스들이 감염이후 자료와 시간표를 원래대로 해놓기때문에 이 방법은 효과가 적다.

주 의

NTFS가 동작하는 Windows NT체계들은 자료흐름을 리용하기때문에 특별히 약하다. 자료흐름은 합법적인 파일과 결합될수 있는 규칙적인 파일이다. 이것은 공격자가 비루스코드를 숨길수 있는 구역을 제공한다. 자료흐름들은 탐색기나 DIR지령으로는 볼수 없다. 자료흐름은 직접(이미 그것의 존재를 알고 있다는 의미) 혹은 자료흐름을 찾을수 있게 설계된 특별한 도구(례하면 www.hoysoft.de/nt/ep-lads.htm에서 내리적재할수 있는 프리웨어인 LADS List Alternate Data Streams)를 리용하여 참고하여야 한다.

스텔스

스텔스는 비루스가 파일이나 기동분구에 만들어 놓은 조작을 숨기게 한다. 비루스가 기억기안에 들어 가면 파일과 디스크분구들에 만들어 진 체계호출들을 관리한다. 호출이 들어 오면 비루스는 호출을 만드는 과정으로 돌아 가는 정보를 수정하여 감염되지 않은것처럼 보이게 한다. 이것은 비루스가 검사를 피할수 있게 한다.

실례로 많은 기동분구비루스들은 스텔스능력을 가지고 있다. 만일 감염된 디스크로 기동한다면(그 결과로 비루스가 기억기에 들어 오면) FDISK와 같은 프로그람들은 기동기록이 정상이라고 보고하게 된다. 이것은 그 비루스가 FDISK로부터의 분구호출을 가로막고 원래의 기동분구정보를 보내기때문이다. 그런데 깨끗한 플로피디스크로 체계를 기동한다면 그 구동기는 접근불가능하게 된다. FDISK를 다시 실행하면 프로그람은 구동기의 기동분구가 감염되였다는것을 알수 있다.

잠복은 또한 DIR나 MEM과 같은 지령이 알려 주는 정보를 위조해서도 실현할수 있다. 이것은 제한된 기억구역안에서 비루스가 자기의 존재를 숨기게 한다. 그런데 스텔스를 리용하자면 비루스가 기억기안에서 동작하여야 한다. 이것은 비루스의 스텔스부분이 반비루스에 약하다는것을 의미한다.

대항책들

일부 비루스들은 검사에 피하기 위하여 대항기능을 가지고 있다. 이 비루스들은 체계에서 비루스주사가 시작되는가를 감시하며 자기들이 검출되지 않았다는것을 검증하기 위한 방어측정을 한다.

이것도 스텔스속성처럼 생각할수 있다.

실례로, 일부 비루스들은 기억기에서 능동으로 되면 체계활동을 조종한다. 만일 비루스가 비루스스캐너가 기동되였다는것을 알아 차리면 다른 비루스가 그 체계에 이미 있는것처럼 속이기 위하여 시도한다. 그렇게 되면 비루스가 실제적으로 존재하지 않아도 체계자원을 파괴하는 어떤 형태의 청소를 실행하도록 한다. 그리고 그 비루스는 파일체계에 잠복하여 새로운 형태의 감염을 일으키게 된다.

스텔스와 마찬가지로 대항책은 비루스가 기억기안에서 동작할 때 활동을 조절한다. 따라서 깨끗한 기동디스크로부터 체계를 기동하는것이 중요하다.

DOS체계에서 체계를 정확히 전원재기동하는것이 필요하다. 많은 비루스들은 CTRL+ALT+DEL 지령을 없애 버리고 틀린 기동을 만들수 있다. 이것은 체계가 재시동하는것처럼 보여도 비루스는 기억기상에서 그냥 동작하게 한다.

암호화

비루스제작자들은 암호화의 쓸모를 홀시하지 않는다. 암호화는 비루스작성자들이 징후체계호출과 프로그람안의 본문렬을 숨길수 있게 한다. 비루스코드를 암호화하여 비루스작성자들은 비루스의 검사가 훨씬 더 힘들어 지게 한다.

그런데 많은 비루스들이 단순한 형태의 암호화를 리용하고 모든 비루스코드에 같은 열쇠를 리용하기때문에 검사는 불가능하지 않다. 이것은 정확한 비루스코드를 내보내기는 힘들지만 복호화된 렬은 모든 파일들에서 같다는것을 의미한다. 만일 복호화열쇠가 깨여 지면 이것은 모든 형태의 비루스들을 검사하는데 리용될것이다. 복호화열쇠가 깨여지지 않는다고 해도 암호문렬은 반비루스프로그람이 비루스검사에 리용할수 있는 징후자료로 된다.

암호화된 비루스들을 검출하는 이 방법의 효과성은 암호화된 결과에 의존한다. 그런데 반비루스프로그람은 자기가 암호화된 정보를 찾는지 아니면 평문정보를 찾는지 모른

다. 만일 암호문렬이 코드의 어떤 형태를 닮았다면 반비루스프로그람은 감염된 파일과 감염되지 않은 파일을 갈라 보기 힘들것이다.

다형성돌연변이

다형성돌연변이비루스는 파일이 감염될 때 비루스흔적을 변화시키는 능력을 가지고 있다. 많은 비루스스캐너는 징후자료코드를 찾아서 비루스를 검사한다.

다형성돌연변이비루스는 감염될 때마다 자기의 형태를 변화시키기때문에 검사하기가 매우 힘들다.

다형성돌연변이비루스를 만드는 한가지 방법은 여러가지 복호화방법을 가진 암호화도식을 리용하는것이다. 임의의 비루스에서는 이 복호화방법들중에서 하나만을 쓴다. 반비루스스캐너는 복호화방법들을 모두 알고 있지 못하는 이상 비루스의 모든 형태를 검출할수 없다.

비루스가 암호화과정에 우연열쇠나 렬을 리용할 때 이것은 거의 불가능하다. 실례로 많은 비루스들은 사용되지 않는 코드들을 가지고 있는데 그것들은 암호화가 되기전에 비루스의 능력에는 영향을 주지 않으면서 그 비루스안의 임의의 위치에 있을수 있다. 이 과정에 만들어 진 암호렬은 그 코드렬이 변하는것으로 하여 매 비루스생성에 따라 달라질것이다.

다형성비루스를 만드는 가장 효과적인 방법은 돌연변이엔진이라고 하는 대상모듈안에 걸개(hook)를 포함시키는것이다. 이 엔진은 모듈화되였기때문에 임의의 비루스코드에 쉽게 붙일수 있다. 돌연변이엔진은 우연수발생기를 가지고 있어 암호문렬을 더욱 복잡하게 만들수 있다.

우연수발생기가 쓰인것으로 하여 출구된 암호문은 가늠하기 힘들며 파일이 감염될 때마다 바뀐다. 이것은 비루스검사를 거의 불가능하게 한다.

폭 탄

이제는 비루스가 성과적으로 복제되고 검사도 피하였다. 이때 다음과 같은 문제가 제기된다.《다음에 비루스는 무엇을 하는가？》대부분의 비루스는 특정의 사건을 기다리도록 설계되였다. 이것은 지정된 날자나 감염된 파일의 지정된 개수 지어 미리 정의된 활동의 개시 등 거의 모든것이 될수 있다.

이러한 사건이 일어 나면 비루스의 진짜 목적이 나타난다. 그것은 콤퓨터의 고성기로 흘러 나오는 친절한 말일수도 있고 하드디스크에 보관된 모든 정보를 지워 버리는 파괴적인것일수도 있다.

대부분의 폭탄들은 현재의 DOS나 Windows환경에서 조작체계와 그것들이 돌리는 프로그람들사이를 명백히 분리하지 않고 있는것으로 하여 해독적인 작용을 할수 있다.

비루스는 낮은 준위의 기능들에 직접 접근할수 있는데 이것은 조작체계가 응용프로그람들의 기능한계를 엄격히 제한하지 않고 있는데로부터 가능하다.

실례로 DOS와 Windows응용프로그람은 직접 기억기를 지적하거나 중단표에 접근할수 있다. 이것은 응용프로그람이 조작체계가 지원하는 기능을 리용하지 않고 응용프로그

람이 직접 그러한 기능을 수행하게 함으로써 그것의 성능을 높일수는 있지만 비루스가 스텔스를 리용할수 있게 하는 기능을 제공하는것으로도 된다.

그러나 폭탄이 할수 있는 일에는 한계가 있다. 폭탄은 콤퓨터를 사용할수 없게 만들수는 있지만 콤퓨터의 임의의 요소들에 물리적손상을 줄수는 없다.

이것은 최악의 경우에 콤퓨터상의 모든 자료를 완전히 지워 버리고 처음부터 시작하면 된다는것을 의미한다. 적어도 하드웨어는 그대로 남아 있으므로 비루스만 제거하면 된다.

속이기

때로 사회적속임비루스라고도 하는 속임은 실제적인것처럼 피해를 준다. 사회적속임비루스는 그것이 콤퓨터가 아니라 감염시키려는 사람에 의거한다는것을 내놓고는 보통의 비루스와 류사하다.

사회적속임비루스의 한가지 실례는 여러해동안 인터네트에 퍼져 있던 Good Times 속임비루스이다.

이 전자우편통보문은 위험한 비루스가 전자우편을 통하여 퍼지고 있다는것을 방송하며 콤퓨터의 모든 파일들을 지워 버릴수 있는 능력을 가진다. 이 통보문는 지어 그 비루스의 존재가 AOL(비루스에서 세계적권위자라고 알려 져 있는)에 의해 확인되였다고 주장한다.

자기 동료들이 이 비루스에 의해 공격 당했을수 있다고 생각하는 사람들은 이때 자기 주소책에 있는 모든 사람들에게 이 속임수를 보내게 된다.

어떻게 사회적속임비루스를 진짜비루스로 볼수 있겠는가?

복제 이 비루스들은 좋은 의도에서 다른 사람의 체계에 자기의것을 복제해 놓는 사람의 습관에 기초하고 있다. 사람들은 습관상 비루스에 대한 경고나 죽어 가는 어린이의 호소로 보이는 전자우편 같은것들을 쉽게 펼쳐볼수 있으며 그 과정에 다른 콤퓨터사용자들에게로 퍼진다. 또한 읽고 있는것을 그대로 믿고 정보를 정확히 확인하려고 하지 않으므로 고의적이 아니지만 그 비루스를 전파하게 된다.

잠복 위협을 숨기기 위해서 이 비루스는 보통 사용자들이 믿을수 있는 통보문들을 만들게 된다. 실례로 그 통보문들은 AOL, IBM, Microsoft와 같은 회사들이 언급된 비루스의 존재를 확인하였다고 주장할수 있다. 이 회사들은 보통 사용자들에게 잘 알려 진 콤퓨터관련기업들인것만큼 통보문은 가치가 있어 보인다.

폭탄 이것은 대부분 사람들이 보통 생각지 않는 부분이다.
《폭탄》은 대역너비의 랑비이며 필요 없는 공포이다.
통보문이 속임이므로 대역너비는 그것이 전파될 때마다 랑비되는것으로 된다. 발송자가 통보문이 긴급함을 가정하였으므로 비루스는 보통 여러 사람에게 발송된다.
통보문은 보통 재난경고가 무시된다고 해도 그것을 포함하게 되므로 불필요

한 공포가 생기게 된다(실례로 사용자의 콤퓨터가 속임비루스에 의하여 감염되였거나 암에 걸린 어린이가 치료비를 보장하겠다는 전자우편들을 받지 못하여 죽었다는 등). 이러한 공포는 추가적인 스트레스와 근심을 더해 주게 된다. 폭탄은 이렇게 콤퓨터자원과 그 자원의 조작자(사람)에게 영향을 미치게 된다.

비루스스캐너는 사회적속임비루스들을 검출할수 없다. 오직 교육과 정보확인만이 이 비루스들이 퍼지는것을 막을수 있다.

주 의

사회적속임비루스의 놀라운 원천은 www.Vmyths.com에 위치한 Computer비루스 Myths홈페지이다.

웜

콤퓨터웜은 상시적인 망접근 혹은 전화접근으로서 자기자체를 복제할수 있는 프로그람이다. 콤퓨터하드디스크나 파일체계에 숨어 있는 비루스와 달리 웜은 자체유지(self-supporting)프로그람이다. 전형적인 웜(Worms)은 능동기억기에서 자기자체를 복제하는 기능만 가지며 디스크에 자기자체를 쓰지 않는다.

웜에는 2가지 종류가 있다. 첫번째 종류는 단 하나의 콤퓨터에서 동작하는것이 있는데 이것은 전형적인 응용프로그람과 비슷하다. 이 웜은 다른 체계에 자기를 복제하거나 정보를 중계하기 위하여 체계의 망련결을 통신통로로 리용한다. 웜의 종류에 따라서 새로운 호스트에로 복제될 때 원래체계에 자기자체를 복제해 둘수도 있고 그렇지 않을수도 있다.

두번째 종류는 망련결을 신경체계로 리용하여 여러개의 체계에서 서로 다른 코드토막들이 돌아 가게 할수 있다. 이 모든 토막들의 활동을 조정하는 중심마디(《뇌수》의 한 종류)가 있는데 이 웜을 Octopus라고 한다.

주 의

웜이라는 말은 1975년에 John Brunner가 창작한 소설 《Shock wave Rider》로부터 유래되였다. 소설의 주인공은 독재정부의 콤퓨터망을 파괴하기 위하여 《tapeworm》이라는 프로그람을 리용한다. 이 프로그람은 정부의 권력기관을 흔들어 놓고 그의 영향하에 있던 사람들을 해방시켰다. 이 소설이 발표되기전에는 이러한 프로그람을 서술한 일반적인 이름이 없었다.

Vampire웜

웜이 항상 나쁜것으로만 간주되였던것은 아니다. 1980년대에 Xerox회사의 John shock와 Jon Hepps는 어떻게 하면 유익한 웜을 만들수 있겠는가에 대하여 연구하였다. 연구결과 그들은 수많은 웜프로그람들을 만들어서 이것을 Xerox망의 관리에 리용

하였다.

가장 효과적인것은 Vampire웜이였다. 이 웜은 체계가 만가동하는 낮에는 휴식하고 밤이 되면 놀고 있는 CPU시간을 리용하여 복잡하고 집약적인 과제들을 처리하였다. 다음날 아침에 웜은 자기의 일을 기억시키고 다시 잠든다.

Vampire웜은 매우 효과적이였지만 콤퓨터체계를 파괴하군 하였다. 체계가 재시동될때 그것들은 웜에 의하여 파괴되였다. 이로 하여 웜들은 모든 망체계들로부터 제거되게 되였다.

큰 인터네트웜

1988년 11월 3일에 큰 인터네트웜이 발견되였다. 6시간도 못되는 사이에 이 99행짜리 프로그람은 인터네트에 련결된 6000개의 Sun과 VAX체계들을 못 쓰게 만들었다.

이 프로그람은 그 시기 국가의 가장 높은 급의 보안전문가의 아들이였던 Robert Morris에 의하여 만들어 졌다. 웜을 고의적으로 악한 마음을 먹고 만들지는 않았지만 아들의 이러한 행동은 아버지의 영상을 흐려 놓았다. 이 프로그람은 의도적으로 파괴기능을 수행하지는 않는다. 웜이 하는 일은 자기가 맞다드는 매 기계의 배경에서 동작하는 작은 프로쎄스를 시동시키는것이다. 이 실험은 하나의 작은 프로그람고장이 아니였다면 아마 주목되지 않았을것이였다. 하나의 호스트를 감염시키기 전에 웜은 그 체계가 이미 감염되였는가를 검사하지 않는다. 이것으로 하여 체계들이 다중으로 감염되였다. 하나의 웜은 그리 크지 않은 처리기부하를 가지지만 수십,수백개의 웜들이 돌게 되면 체계는 자기의 기능을 못하게 된다.

관리자는 자신이 전투에서 패했다는것을 알았다. 체계를 청소하고 재시동하여도 그것은 다시 빨리 감염되였다. 그 웜들이 하나의 체계로부터 다른 체계로 움직일 때 SendMail취약성을 리용하고 있었다는것이 알려 지자 많은 관리자들은 인터네트련결을 끊거나 또는 자기들의 우편체계를 차단해 버렸다.

이것은 오히려 더 불리하였다. 왜냐하면 이렇게 하면 감염을 막는 정보를 포함한 웜에 대한 모든 새로운 정보들로부터 그 싸이트를 격리시키기때문이다. 이 사건들로부터 시작된 모든 혼돈상태들에 의해서 많은 좋은것들도 제기되였다. 체계의 취약성에 대한 사람들의 생각을 변경시키기 위하여 이러한 이야기를 써먹기도 하였다. 그때 이러한 취약성들은 그저 작은 결함으로 간주되였다. 결국 이 사건으로 하여 콤퓨터관련보안문제들을 기록하고 방조하는 조직인 콤퓨터긴급응답기구(Computer Emergency Response Team(CERT))가 출현하게 되였다.

WANK웜

인터네트웜이 잘 알려 져 있기는 하지만 그것이 가장 나쁜 웜은 아니다. 1989년 10월 WANK(Worms Against Nuclear Killers)웜이 믿을만한 체계상에 출현하였다. 이 웜은 강한 파괴력을 가지나 DEC체계와 DECnet규약을 리용하는 체계만을 감염시킨다. 이 웜의 파괴작용은 다음과 같다.

- 리용하는 가입등록이름과 통과암호를 통하여 어느 체계에 침투하였는가를 알

리는 전자우편을(대체로 웜의 제작자에게) 보낸다

- 현존 구좌의 통과암호를 변경시킨다
- 체계에로 들어 가는 보충적인 함정문접근을 남긴다
- 우연적인 마디우의 사용자들을 발견하고 그들에게 전화설비를 리용하여 전화를 건다
- 국부COM파일들을 감염시켜 웜을 체계에서 지운다고 해도 후에 재시동할수 있게 한다
- 체계가 《WANKed》되였다는것을 보여 주는 알림기발을 변화시킨다
- 가입스크립트를 수정하여 모든 사용자파일들이 지워 진것처럼 나타나게 한다
- 가입등록후에 사용자파일들을 숨김으로써 사용자가 파일들이 지워 졌다고 생각하게 한다

우에서도 알수 있는바와 같이 이 비루스는 파괴력이 세다.
감염된 체계로부터 이 웜을 성과적으로 제거하려면 오랜 시간이 걸린다.

IRC웜

오늘날 보다 일반적인 형태의 적대적인 웜은 IRC(Internet Relay Chat)웜이다. 이 웜들은 mIRC통신쏘프트웨어를 리용하는 모든 사용자들에게 영향을 준다. 사용자가 특정한 IRC통로를 리용하면 이 웜은 사용자의 체계를 감염시킨다. 그다음 가만히 숨어서 IRC통로관계자들이 알고 있는 열쇠단어를 보내기를 기다린다.

매 열쇠단어는 어떤 형태의 특정한 작용을 유도해 내도록 설계되였다. 실례로 한 열쇠단어는 UNIX를 돌리는 대상에 대하여 설계되였다.

열쇠단어가 지나가면 웜은 국부 통과암호파일의 복제를(mIRC의 DCC지령을 리용하여) 그 지령을 보낸 IRC사용자에게 보낸다.

또 하나의 열쇠단어는 Windows 95/98 사용자용으로 설계되였는데 그것은 등록고의 하나의 복제를 전송한다. 또 다른 하나의 열쇠단어는 그 지령을 보낸 사람에게 모든 감염된 체계들의 국부하드구동기에 대한 완전한 읽기 및 쓰기허가를 준다.

마크로웜

마크로비루스와 류사하게 마크로웜들은 자기의 실행환경으로써 VBA와 Microsoft응용프로그람들을 리용한다. 마크로웜은 Outlook 또는 Outlook Express에 기억된 매 전자우편주소에 불쾌감을 주지 않는(그러나 호소적인) 이름으로 자기의 복제를 전송한다. 이 웜은 사회적심리에 의존하며(실례로 《I Love You》와 같은 이름으로) 그 웜을 실행할 수신자를 끌어 들이기 위하여 Outlook의 기정의 구성(파일이름의 확장자를 숨기는)에 의존한다. 이러한 웜들의 성과로 하여(일명 I Love You 웜을 포함) 일부 프로그람제작자들은 웜이 아니라 비루스에 가까운 혼성프로그람을 만들어서 파일들을 지우고 조작체계가 제대로 동작할수 없게 만든다.

트로이목마

트로이목마는 이름이 보여 주는것처럼 불쾌하지 않거나 또는 훌륭한 패키지안에 어떤 나쁜 놀라운것을 숨겨 놓는 응용프로그람그람이다. 그 놀라운것이란 트로이목마의 작성자가 만들어 놓는 프로쎄스 또는 함수인데 그것들은 사용자가 알지 못하는 그리고 좋아하지 않는 그러한 기능을 수행한다. 응용프로그람을 숨기는것이 바로 트로이목마이다.

트로이목마는 왜 비루스가 아닌가

트로이목마는 복제되거나 자체로 다른 파일들에 붙지 않는다는 점에서 비루스와 다르다. 트로이목마는 자기의 원래의 원천코드안에 폭탄을 가지고 있는 독립적인 응용프로그람이다. 그것은 또 하나의 응용프로그람의 효과에 의하여 악의적인것으로는 되지 않는다.

실례로 현존하는 망응용프로그람들을 교체하기 위하여 만들어 진 많은 UNIX트로이목마들이 있다. 공격자는 telnet봉사기프로쎄스(telnetd)를 자기가 만든것으로 바꾸어 놓을수 있다. 이 프로그람은 표준telnetd프로그람과 꼭같이 동작하지만 그 체계에서 인증되는 모든 가입등록이름들과 통과암호들을 기록한다. 반대로 공격자는 telnet의뢰기응용프로그람을 교체하여 원격체계에 대한 구좌정보들을 얻을수 있다. 이렇게 되면 그는 망의 매봉사기에 체계적으로 침투할수 있게 된다.

공격자는 또한 파괴의 목적에서도 트로이목마를 설계한다.

실례로 1997년 4월에 많은 사람들이 AOL4FREE.COM트로이목마의 피해를 입었다. 사용자들은 AOL우에서 무효로 리용할수 있는 파일을 찾았다고 생각하고 그것을 체계의 국부하드구동기에 받아 들였다. 그런데 프로그람이 태워 지자마자 C구동기에 있는 모든 파일들을 지웠다.

트로이목마들의 가장 성공적인(일반적인) 공격목표는 Windows 95/98 또는 Windows NT/2000의 전화련결망을 리용하는 사용자들이다. 이 트로이목마들은 사용자들을 유혹할수 있는 많은 편의프로그람들을 가지고 있다. 만일 그것을 설치하면 트로이목마는 사용자의 전화번호책을 샅샅이 뒤져 보고 Windows전화련결망의 캐쉬의 복제본을 알아 낸다. 다음 Windows API의 호출을 리용하여 이 정보들을 트로이목마의 제작자에게 전자우편으로 보낸다. 공격자는 국부체계접근과 함께 다른 체계들을 공격하는데 리용할수 있는 정당한 ISP구좌정보를 얻는다.

바로 내가 트로이목마를 구입하였는가

물론 모든 트로이목마들이 다 진짜 공격자들에 의하여 만들어 지는것이 아니다. 실례로 일부 사용자들은 자기가 Microsoft망을 리용할 때 그 쏘프트웨어가 체계하드웨어와 쏘프트웨어의 완전한 목록을 만든것을 보고 놀란다. 여기에는 Microsoft의것과 경쟁자의 제품들도 포함되여 있다. 사용자가 그 망에 련결할 때 이 정보가 자동적으

로 Microsoft에 전송되게 된다. Microsoft는 기술적리용만을 위하여 이러한 정보들을 수집하고 있다고 주장하지만 많은 사람들은 그것이 명백한 개인비밀의 침해로 여기고 있다.

회사들에서 사용자의 보안상태를 침해하는 기능을 추가하는 경우가 많다. 실례로 1998년 5월 3COM에서 다른 많은 망하드웨어회사들과 마찬가지로 자기의 교환기와 경로기제품들에로의 접근을 위한 《뒤문》구좌를 가지고 있다는것이 공개되였다. 이러한 문서화되지 않은 구좌들은 말단 사용자들에게 보이지 않으며 지워 지거나 무효로 만들수 없다.

제작자는 기술적인 리유로 이런 《뒤문》을 만들었다고 주장하지만 이것은 제품의 영상을 흐리게 하고 관리자들을 신용할수 없게 한다.

이러한 활동들은 기술적유지와 트로이목마사이의 흐린 구역에 존재한다. 이러한 문서화되지 않은 《뒤문》이 이름난 회사들에 의하여 만들어 지지만 이것들은 보안을 약화시키며 고객들로 하여금 잠재적인 손실에 대하여 알지 못하게 한다.

명백히 《뒤문》접근은 많은 관리자들이 금지하려고 하는것이지만 그들은 우선 그것이 존재한다는것부터 알아야 한다.

방 지 방 법

이러한 나쁜프로그람들에 대하여 무엇을 할수 있는가? 나쁜프로그람을 알아 내는 확고한 방법은 능력 있는 프로그람작성자가 원천코드를 검사해 보는것이다. 대부분의 응용프로그람들이 이미 실행방식으로 되여 있으므로 체계우의 매 파일을 한걸음씩 조사하여야 한다. 그런데 이것은 많은 시간과 비용을 요구한다.

이런것을 생각해 볼 때 임의의 다른 예방대책들의 효과성은 적다. 정확히 얼마나 많은 보안이 자기에게 필요한가를 결정하기 위하여서는 위험을 분석해 보아야 한다. 감염을 막기 위한 여러가지 기술들이 있다. 이 매개는 우점과 함께 약점도 가지고 있기때문에 세가지 또는 그 이상의 기술들을 결합하는것이 가장 좋다.

접근조종

접근조종방책을 확립하는것은 좋은 보안대책뿐아니라 나쁜프로그람들의 전파를 막게 한다. 접근조종을 감염된 프로그람에 의하여 쉽게 변화될수 있는 파일속성(읽기전용 또는 체계파일 등)과 혼돈하지 말아야 한다. 진짜접근은 체계관리자로 하여금 사용자-사용자준위에서 파일허가준위를 설정하게 하는 다중사용자조작체계를 통하여 관리되여야 한다.

접근조종은 나쁜프로그람의 존재를 검출하거나 지우지 못한다. 이것은 체계의 감염을 막을수 있게 도와 주는 한가지 방법에 불과하다. 실례로 대부분의 비루스들은 감염된 기계에 의하여 모든 파일들에 대한 완전한 접근을 가진다(Windows NT에서의 기정의 허가와 같은).

유능한 관리자들은 이러한 기정의 허가들을 변경시켜 사용자들이 자기들의 실행가능

한 프로그람들에 대하여 읽기권한만을 가지도록 하여 비루스가 파일들을 감염시킬수 없게 한다.

주　의

그런데 이것은 모든 실행파일에 대하여 다 동작하지는 않는다. 일부는 실행기간에만 자기자체를 수정할것을 요구한다. 사용자들은 이 실행파일들에서의 쓰기접근을 요구하며 관리자는 시간과 자료표가 규칙적으로 변화될것을 기대할수 있다. 어느 실행파일이 쓰기접근을 요구하는지 어떻게 아는가? 보통 모른다. 어느 실행파일이 자기의 날자와 시간표를 변경시키며 쓰기접근이 제공되지 않을 때 깨여 지는가 하는것은 시행착오적문제이다. 그런데 이러한 자체쓰기실행파일들은 드물다. 이러한것들을 자주 실행시키지 말아야 한다.

검열합확인

검열합 또는 순환여유검사(CRC)는 파일자료의 수학적인 검사이다. 이것은 파일의 내용을 수량으로 표시한다. 파일에서 자료의 한 바이트가 변하면 파일의 크기가 변하지 않았다고 해도 검열합값이 변한다. 먼저 감염되지 않은 체계의 기준값이 만들어 진다. 그다음 파일의 변화를 감시하기 위하여 CRC가 규칙적인 주기로 수행된다.

이 방법에는 두가지 약점이 있다. 첫째로, CRC가 파일의 감염을 정확히 검사할수 없다는것이다. 이것은 자체쓰기실행파일들이 규칙적으로 검열합확인을 진행할수 없다는것을 의미한다. 또한 변화가 정확히 비루스에 의한것이라고 하더라도 CRC는 파일은 청소할수 없다. 둘째로, 많은 비루스들이 CRC로서 파일의 정보가 변하였다는것을 알수 없게 작성한다는것이다.

일러두기

CRC가 비루스를 검사하는 가장 효과적인 방법은 아니지만 트로이목마의 교체를 발견하는데서 큰 도움을 줄수 있다. 현존의 인증봉사(telnet 또는 FTP의뢰기 그리고 봉사기쏘프트웨어와 같은)를 교체하도록 설계된 트로이목마는 현존의 파일들을 변경하는것이 아니라 그것들을 교체한다.

이 파일교체는 검열합확인에 의하여 나타난다. 그런데 비루스스캐너는 이 문제를 완전히 놓치고 파일이 임의의 비루스코드를 포함하지 않고 있다고 통보한다. 이것은 트로이목마를 인증하는데서 CRC가 훨씬 효과적이라는것을 말해 준다.

과정감시

나쁜프로그람이 체계에 침습하는것을 막는 방법에는 과정감시도 있다. 과정감시는 여러가지 체계활동을 관찰하고 수상하다고 보이는 모든것을 차단한다. 실례로 대부분 현대콤퓨터들의 BIOS는 반비루스설정을 포함하고 있다.

이 설정은 콤퓨터가 1차기동레코드에로의 모든 쓰기시도를 차단할수 있게 한다. 만일 기동분구비루스가 이 구역에 자기자체를 복제하려고 하면 BIOS는 그 요구를 차단하고 사용자의 접근을 요구한다.

여기에는 또한 몇가지 문제가 있다. 첫번째 문제는 비루스가 보통 프로그람들과 비슷한 속성들도 가지고 있다는것이다. 즉 이 두개를 구별해 보는것이 매우 어려울수 있다. 실례로 FDISK를 실행하면 BIOS비루스통보를 내보낸다. FDISK가 비루스가 아니라고 해도 그것의 활동이 수상하기때문에 경고를 내보낸다. 이것은 틀린 긍정이라고 하는데 BIOS는 사실은 비루스가 아니지만 비루스를 검사했다고 생각한다.

두번째는 과정감시에 관한 문제 즉 사용자간섭과 숙련을 요구한다는것이다. 실례로 틀린 긍정을 받은 사용자는 콤퓨터에 완전히 정통하여 진짜비루스가 실제로 검출되지 않았고 FDISK의 정상적인 동작이 경보를 발생시켰다는것을 알수 있어야 한다.

그러나 FDISK가 기억된 플로피디스크우에 기동분구비루스가 있을수 있다. 이것은 사용자가 정확히 비루스가 있을 때 틀린 긍정이 통보된다고 가정할수 있게 한다. 이것은 검사과정의 서로 다른 점에서 BIOS비루스경보를 내지만(FDISK가 끝날 때가 아니라 적재될 때) 말단사용자는 이 비루스문제를 정확히 식별할수 있으리만큼 높은 수준의 숙련이 있어야 한다.

비루스와 보통 프로그람을 구별하는 문제는 다른 형태의 동작을 관리하려고 할 때보다 중요한 문제로 제기된다. 파일지우기가 의심스러운것으로 간주되는가? 파일관리프로그람이 파일들을 지울 때마다 틀린 긍정들을 발생시킨다. 파일변화와 기억기변경 등을 관리하려고 할 때에도 같은 현상이 일어 난다.

이러한 활동들은 모두 비루스에 의하여 수행될수도 있고 보통 응용프로그람에 의하여 수행될수도 있다.

유일하게 쓸모 있는 과정감시는 앞에서 언급된 BIOS비루스경고이다. 사실상 틀린 긍정경고가 생길 때 사용자가 FDISK나 또는 합법적으로 기동분구에 쓰기를 시도하는 다른 응용프로그람을 실행하고 있는 경우는 매우 드물다.

이러한 현상은 사용자가 새로운 조작체계를 설치할 때 생긴다. 이것은 틀린 긍정의 발생이 최소로 될수 있다는것을 의미한다.

비루스스캐너

비루스를 검사하는 가장 일반적인 방법은 비루스스캐너쏘프트웨어를 리용하는것이다. 비루스스캐너는 감염된 파일에 들어 있는 비루스를 확정하기 위하여 증거파일들을 리용한다. 증거파일은 모든 알려 진 비루스와 그것의 특별한 속성들을 기록한 자료기지이다. 이 속성들은 매 비루스코드의 실례와 그 비루스들이 감염시키는 파일의 형태 그리고 비루스를 찾는데 도움을 줄수 있는 임의의 다른 정보들을 포함한다. 이러한 정보가 들어 있는 여러가지 파일들을 리용하여 이 쏘프트웨어를 계속 갱신함으로써 가장 최근의 비루스들도 검출할수 있다. 그러나 전체 프로그람을 갱신하지는 말아야 한다. 이것은 매달 많은 새 비루스들이 검사되기때문에 여전히 쓸모 있다.

비루스스캐너가 파일을 검사하면 파일의 임의의 코드가 증거파일의 임의의 부분과

같은가 본다. 같은것이 있으면 사용자는 비루스가 검출되였다는것을 알수 있다. 그다음에 대부분의 스캐너들은 비루스를 청소하는 특별한 처리를 진행할수 있다.

비루스스캐너의 가장 큰 약점은 알려 진 비루스들만을 검출할수 있다는것이다. 새로 만들어 진 비루스에 대하여 실행시키면 스캐너는 그것을 놓칠수 있다. 이것은 다형성문제를 취급할 때 특별히 곤난한 문제로 된다. 이 장의 《다형성돌연변이》에서 언급한바와 같이 다형성비루스들은 자기의 흔적을 매 감염때마다 변화시킬수 있다. 이러한 형태의 비루스에 100% 효과적인 비루스스캐너로 되자면 모든 가능한 다형성치환을 기록한 증거파일이 있어야 한다. 하나의 치환을 놓쳐도 비루스스캐너는 감염된 파일을 제거하지 못할수 있으며 비루스는 다시금 체계를 감염시킬수 있다.

일러두기

비루스스캐너를 선택할 때 여러가지 많은 비루스들을 검사할수 있을뿐아니라 많은 다형성비루스들도 검사할수 있는가를 보아야 한다.

압축되거나 암호화된 파일들도 비루스스캐너에 문제를 일으킬수 있다. 이러한 처리들이 정보를 재배치하기때문에 비루스스캐너는 파일에 숨어 있는 비루스를 검사할수 없다.

실례로 PKZIP를 리용하여 많은 파일들을 압축하여 플로피디스크에 넣는다고 하자. 비루스스캐너를 리용하여 디스크를 검사할 때 비루스를 포함한 파일들은 검사되지 않는다. 비루스스캐너가 ZIP파일형식을 리해하지 못하는 한(많은 경우 그러하다.) 파일에 숨겨 져 있는 비루스를 검사할수 없다.

암호화된 파일에 대하여서는 이러한 문제가 더 심각해 진다.

비루스스캐너는 암호화된 파일을 복호화할수 없기때문에 많은 비루스들을 놓칠수 있다. 비루스가 없다는것을 확인하자면 파일을 먼저 복호화하고 비루스스캔을 실행하여야 한다.

비루스스캐너의 변종들

비루스스캐너에는 크게 두가지 종류가 있다.

- 요구형
- 기억기상주형

요구형스캐너들은 어떤 수동적인 또는 자동적인 처리에 의해 시동되여야 한다. 요구형스캐너가 동작하면 전체 구동기나 체계에서 비루스를 찾는다. 이것은 RAM기억기와 하드구동기, 플로피디스크와 같은 기억장치들을 포함한다. 기억상주형스캐너들은 체계의 배경에서 동작하는 프로그람들이다. 이것들은 보통 체계의 기동시에 초기화되여 계속 능동으로 남아 있는다. 파일이 접근할 때마다 기억기상주형스캐너는 파일호출을 차단하고 파일을 기억기에 태우기전에 비루스가 없는가 검사한다.

이 방법들은 자기의 우점과 약점을 가지고 있다. 요구형스캐너들은 사건이 제기된 후에야 동작하게 된다. 임의의 파일에 접근하기전에 스캐너를 항상 기동하지 않으면 체계는 검출전에 비루스와 맞다들게 된다. 기억기상주형비루스스캐너는 비루스가 체계를

감염시키기전에 비루스를 잡아 내지만 비용이 든다. 매 파일을 주사하면 체계의 파일접근속도를 낮추며 체계의 응답속도를 떨군다.

기억기상주형비루스스캐너의 제작자들은 파일접근속도가 중요하며 많은 사용자들이 큰 부하가 걸리는 스캐너보다는 좀 기능이 낮은 스캐너를 요구한다는것을 알고 있다. 이러한 리유로 하여 많은 기억기상주형스캐너들은 요구형스캐너만큼 기능이 충분하지 못하다.

더 좋기는 제일 많이 발생하는 비루스증거들을 검출하거나 제일 감염 받기 쉬운 (COM파일과 같은) 파일들을 주사하는것이다.

일러두기

좋은 보안형태는 요구형과 기억기상주형비루스스캐너를 다같이 리용하는것이다.

큰 환경에서의 문제들

모든 비루스스캐너들은 주기적으로 증거파일들을 갱신하여 자기들의 제품이 가능한껏 많은 알려 진 비루스들을 검사할수 있게 한다. 증거파일들을 갱신하는것은 큰 망환경을 책임진 체계관리자들에게 부담을 준다. 만일 DOS나 Windows, Macintosh조작체계를 탁상용콤퓨터에서 실행한다면 매 체계우에서 증거파일을 갱신하여야 한다.

많은 제작자들은 이 문제를 수정하기로 하였다. 실례로 Intel회사의 LANDesk Virus Protect는 여러개의 봉사기들과 탁상용콤퓨터들을 그룹화하기 위하여 비루스령역이라는 개념을 리용한다. 망관리자는 그다음 증거파일들을 갱신하고 경고들을 감시하며 조종화면으로부터 파라메터들을 조종한다. 이렇게 하면 큰 규모의 환경에서 비루스보호에 필요한 작업량을 크게 줄일수 있다.

유연한 비루스보호방법은 전반적인 비용을 줄일뿐아니라 환경을 안전하게 한다. 언급한바와 같이 비루스스캐너제작자들은 주기적으로 증거파일들을 갱신한다. 그러나 이러한 증거파일들은 적게 쓰이거나 설치되지 않는다.

한가지 유연한 방법은 이 증거파일들을 요구하는 모든 체계들에 배포하는것이다.

발견적스캐너

발견적스캐너들은 하나의 파일이 비루스로 볼수 있는 프로그람코드를 포함할 가능성을 결정하기 위하여 통계적인 분석을 진행한다.

발견적스캐너는 비루스스캐너와 같이 코드를 증거파일과 비교하지 않으며 등급체계를 리용하여 분석되는 프로그람코드가 비루스일 확률을 결정한다. 만일 확률이 크면 발견적스캐너는 사용자에게 비루스가 검출되였다는것을 알린다. 대부분의 현대적인 비루스스캐너들은 발견적스캐너능력을 가지고 있다.

발견적스캐너의 가장 큰 우점의 하나는 갱신을 요구하지 않는다는것이다. 파일들이 체계에서 등급이 매겨 져 있기때문에 증거파일들은 비교를 요구하지 않는다. 이것은 발견적스캐너가 이전에는 볼수 없었던 좋은 비루스검출기능을 가지고 있다는것을

의미한다. 이것은 증거파일을 규칙적으로 갱신할수 없는 사용자에게 있어서 대단히 유익하다.

발견적스캐너의 가장 큰 약점은 틀린 긍정들을 내보낼 가능성이 있는것이다. 우에서 언급한바와 같이 모든 비루스코드가 규칙적인 프로그람코드와 다른것은 아니다. 이것은 둘사이를 구별하는것이 매우 어렵다는것을 의미한다. 체계관리자가 만일 존재하지 않는 비루스들을 통지할 가능성이 있는 낮은 급의 발견적스캐너를 배비한다면 체계성능을 떨굴수 있다.

응용프로그람준위비루스스캐너

응용프로그람준위비루스스캐너는 비루스방지의 새로운 종류이다. 비루스로부터 특정의 체계를 보호할 대신 응용프로그람준위비루스스캐너는 특정의 봉사를 안전하게 한다. 례를 들면 전자우편은 파일접근을 통하여 비루스를 전파시킨다. Trend Micro회사는 SMTP중계기로서 동작할수 있는 Inter Scan VirusWall이라고 하는 제품을 제작하고 있다. 들어 오는 우편을 받아들이고 적당한 우편체계에 그것을 보낼 대신 Inter Scan VirusWall은 우편을 내부의 우편호스트에 보내기전에 완전한 비루스주사를 진행한다. Inter Scan VirusWall은 SMTP뿐아니라 FTP와 HTTP의 자료흐름도 주사할수 있다. 이것은 원본파일들뿐만아니라 PKZIP와 같은 많은 기록형식들도 포함한다. 이것은 인터네트로부터 받아 들인 모든 파일들에 적대적인 비루스들이 없다는것을 보증할수 있게 한다.

일러두기

지금 많은 회사들은 현존의 방화벽제품들과 직접 통합되는 제품들을 만들고 있다. 례를 들어 Cheyenne쏘프트웨어회사는 Check Point의 방화벽-1제품을 위한 비루스스캐너를 만들고 있다. 이것은 비루스주사가 망보안을 실현하는 같은 체계우에서 관리될수 있게 한다. 이것은 망관리자에게 보안과 비루스방지를 다같이 관리하는 하나의 관리점을 준다.

비루스보안의 배비

비루스로부터 자기의 망을 지키기 위한 몇가지 배비방법을 보기로 하자.

주 의

이것은 하나의 지도서만을 주며 특정한 요구에 맞게 하려면 그것을 변경하여야 한다.

그림 11-1과 같은 망구조를 보자. 그림은 많은 봉사기조작체계를 리용하는 혼합된 환경을 보여 준다. 탁상용콤퓨터환경도 역시 조작체계들의 혼합을 리용한다. 이러한 환경을 가지고 있는 조직들에 대하여 비루스나 트로이목마, 웜으로부터 보호할 임무가 주어 졌다고 하자. 또한 이러한 과제를 최소의 비용으로 수행하여야 한다고 하자.

망의 구조를 연구하고 어떤 권고안을 만들어야 하는가를 생각해 보시오.

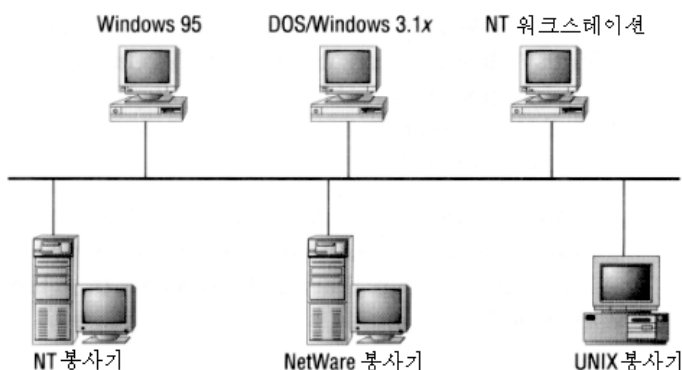



그림 11-1. 비루스방지를 요구하는 망의 실례

탁상형체계의 보호

탁상환경이 여러가지 조작체계들을 리용할 때 하드웨어플래트홈은 일치한다(PC호환). 이것은 모든 탁상체계들이 같은 형태의 비루스들에 감염될수 있다는것을 의미한다. 많은 조작체계를 리용함에도 불구하고 자기의 탁상체계를 가능한대로 표준화하기 위하여 노력하여야 한다.

가능한 BIOS기동분구보호

독자가 할수 있는 가장 효과적인 제의는 체계의 BIOS를 통하여 기동분구보호를 할수 있는것이다. 이것은 모든 체계의 기동분구를 안전하게 하는 빠르고 효과적인 방법이다. 이것은 말단사용자들에게 기동분구경고들이 무엇을 의미하며 사용자들이 그것에 어떻게 대답하겠는가를 교육하여 실현할수 있다.

사용자가 자기의 조작체계를 갱신하지 않는 한 틀린 긍정경고는 문제로 되지 않는다.

요구형스캐너

매 탁상체계는 모든 국부구동기를 규칙적으로 비루스검사하기 위하여 구성한 요구형스캐너를 리용하여야 한다.

만일 탁상체계들이 밤에도 전원이 꺼지지 않을 때 이러한 검사는 밤에 진행되도록 계획할수 있다. 그렇지 않으면(점심시간과 같은) 고정적인 휴식시간에 또는 매주 적당한 시간에 스캐너를 가동시킬수 있다.

요구형스캐너로 모든 국부파일들을 검사하여 비루스가 침습하지 않았거나 또는 불명확한 확장자를 가진 파일을 통하여 침습하였다는것을 확인할수 있다. 물론 적당한 요구형스캐너는 발견적스캐너능력을 포함하여야 한다.

또한 모든 주사결과를 중심위치에 알리는 어떤 방법이 있어서 자료가 체계관리자에게 장악되여야 된다.

기억기상주형스캐너

매 탁상체계들은 또한 체계초기화에서 기억기상주형스캐너를 실행하여 비루스가 국부파일체계에 들어 오거나 기억기에서 실행되기전에 제거하여야 한다. 어느 파일이 기억기상주형스캐너에 의하여 검사되였는가를 지적하고 싶을 때도 있다.

매 탁상체계에 대하여 규칙적인 요구형스캐너를 수행하기때문에 어떤 지연이 생긴다. 가장 일반적인 비루스에 감염된 파일들만을 검사하여 체계성능에 주는 기억기상주형스캐너의 영향을 줄일수 있다. 이것이 보안자세를 약화시킬수 있으나 체계성능에서의 리득은 그 손실을 보상할수 있다.

기억기상주형스캐너는 다음과 같은것을 검사하여야 한다.

- 읽기전용파일
- 웜들
- COM과 EXE파일 같은 실행파일
- Microsoft Word나 Excel 같은 마크로가능한 문서들

파일읽기들을 검사할수 있다. 왜냐하면 디스크에 씌여 진 파일들을 검사하는것은 과부하를 줄수 있기때문이다. 만일 어떤 스캐너가 파일이 기억에 읽어 질 때 비루스를 찾는데서 실패했다면 그 스캐너가 파일이 디스크에 써질 때 비루스를 검출한다는것은 거의 불가능하다. 많은 웜들이 정보를 디스크에 기억시키지 않기때문에 요구형스캐너에 의해 검사되지 않는다. 그러므로 웜들도 검사하여야 한다. 마지막으로 기억기상주형스캐너를 리용하여 감염될 가능성이 큰 파일들을 검사하여야 한다. 여기에는 실행파일뿐만아니라 마크로명령들을 기억할수 있는 파일들도 포함될수 있다.

고려되지 않은 선택안

우리는 파일속성의 설정과 검사합확인에 대하여 언급하지 않았다.

왜냐하면 쉽게 알수 있는바와 같이 이 방법들이 많은 비루스종류들에 대하여 효과가 없기때문이다. 같은 리유로 파정감시의 다른 형태들도 취급하지 않았다(BIOS기동분구경고를 제외하고). 가장 적은 노력으로 높은 준위의 방지를 실현하여야 한다.

한가지 추가적인 선택안은 사용자가 임의의 실행파일에 쓰기접근하는것을 막기 위하여 NT/2000워크스테이션의 파일허가를 리용하는것이다. 이것은 이런 체계들우에서의 비루스감염은 줄이지만 다른 탁상형기계들에서 리용된 표준구성과는 차이난다. DOS와 Windows 95/98/Me가 실제적인 다중사용자조작체계가 아니기때문에 파일체계의 선택된 부분에로의 국부사용자접근을 제한할 길이 없다. 이것은 NT/2000워크스테이션구성이 다른 탁상형기계들과 다르다는것을 의미한다.

또한 이 선택안은 널리 퍼진 일반적인 비루스인 마크로비루스들을 취급하지 않는다. 이러한 비루스들은 문서파일에 숨는다.

이 파일들을 기억하자면 사용자들이 문서기억등록부들에 쓰기접근을 하여야 한다. 이러한것을 생각해 볼 때 이 선택안은 많은 문제점들을 산생시킬수 있다.

NT 및 NetWare봉사기의 보호

NT/2000과 NetWare봉사기들은 자원을 공유하기때문에 탁상형기계들과 다른 보호방법이 필요하다. 이 체계들에서 비루스보호는 훨씬 더 중요하다. 왜냐하면 탁상형기계들사이의 비루스전파에 리용될수 있기때문이다. NT/2000봉사기의 경우 전송만 되는것이 아니라 자기자체를 감염시킬수도 있다.

요구형스캐너

탁상형체계들에서 요구형주사를 실행하여 밤에 모든 파일들을 주사할수 있다. 대부분의 봉사기형비루스스캐너제품들은 이러한 목적으로부터 작성된다. 밤에 주사를 실행하자면 그전에 요구형스캐너가 설정되여야 한다. 이것은 모든 파일들에 비루스가 없다는것을 보증한다.

기억기상주형스캔

Windows NT를 위하여 설계된 기억기상주형스캐너는 봉사기의 기억기와 국부파일체계에 기록된 파일들을 검사한다. 그런데 기억기상주형스캐너는 NetWare봉사기에서 동작할 때 조금 다른 형식으로 동작한다. 이것은 봉사기가 표준실행파일들을 실행할수 없기때문이다. 체계가 파일기억에 리용되기때문에 기억기는 검사할 필요가 없다. 우리가 스캔과 관련하여 가장 관심하는것은 들어 오는 망자료흐름이다.

봉사기에 기초한 기억기상주형스캐너는 다음과 같은것을 검사한다.

- 웜들과 트로이목마들을 위한 국부기억기(NT에서만)
- 망에서 들어 오는 실행파일들
- 망에서 들어 오는 마크로가능문서들

탁상형기계들에서처럼 성능을 개선하기 위하여 최소의 파일검사가 진행된다. 그외에 비루스가 들어 오는것은 밤마다 요구형비루스주사를 실행하여 잡는다.

일러두기

서로 다른 회사들의 제품들을 망의 매 부분을 비루스로부터 보호하는데 리용하면 일부 추가적인 리익을 얻을수 있다. 실례로 봉사기에서는 어느 한 회사의 제품을 쓰고 탁상형기계에서는 다른것을 리용할수 있다. 두개 회사의 증거파일들이 같지 않기때문에 제품들을 혼합 및 비교하여 리용하면 비루스방지에서 최대의 효과를 얻을수 있다.

파일허가

이 장에서 이미 언급한바와 같이 사용자준위의 파일허가를 설정하는것은 실행파일들이 감염되지 않게 한다. 이러한 형태의 리익은 망우에 어떤 응용프로그람이 있는가에 크게 관계된다. 만일 모든 응용프로그람들이 국부워크스테이션에 보관되여 있다면 봉사기에는 읽기전용사용자준위접근을 설정하여 보호하여야 할 실행파일들이 없게 된다. 그러나 모든 응용프로그람들이 하나 또는 두개의 봉사기들로부터 나온다면 요구되는 허가의 최소준위를 설정하여 비루스감염의 가능성을 줄인다.

고려하지 않은 선택안들

과정감시나 검열합확인은 론의하지 않았다. 왜냐하면 이 방법들은 둘다 비루스스캐너쏘프트웨어보다 효과적이지 못하기때문이다.

UNIX체계의 보호

한가지 중요한것을 놓치고 있다. UNIX체계는 무엇에 리용되고 있는가?

그것은 단순한 우편중계기가 아니다. 이 질문에 대한 대답은 독자의 선택안에 큰 영향을 줄수 있다.

실례를 들어 C코드를 콤파일하기 위한 공학적체계를 가정하자. 사용자들은 체계에 telnet와 FTP를 통하여 련결된다.

일러두기

론리적인 결정을 할수 있는 충분한 정보가 있는가를 항상 확인하여야 한다.

파일의 무결성검사

UNIX체계와 관련하여 가장 큰 관심사중의 하나는 누군가가 인증정보를 얻기 위하여 체계에 트로이목마를 태우려고 시도할수 있다는것이다. telnet봉사기를 다른것으로 바꾸어 놓음으로써 공격자는 체계를 인증하는 매 사용자들로부터 가입등록정보를 얻을수 있다.

이러한 활동을 검사하는 가장 간단한 방도는 규칙적으로 파일완전성을 검사하는것이다. 이것은 CRC검사를 포함하여 원래 파일과 크기가 같은가 또는 시간표를 가진 변화도 검사할수 있다. 들어 오는 련결을 받아 들이는 임의의 다른 처리와 함께 telnet와 FTP봉사기도 검사하여야 한다. 이 검사는 서로 다른 기계들에서도 분석할수 있게 자동적으로 실행되여야 한다. 서로 다른 기계우에서의 결과를 분석하여 체계를 손상시키려는 시도들을 막을수 있다.

과정감시

UNIX기계와 관련된 또 다른 문제는 체계에 웜을 리용하여 침입할수 있다는것이다. 이것은 체계에서 동작하는 새로운 처리를 요구한다. 완전성검사에서와 같이 하나의 개별적인 체계에 대한 결과를 검열하고 분석하여야 한다. 체계에서 무엇이 동작하는가를 알면 새로운 처리가 나타날 때 해당한 처리를 할수 있다.

파일허가

기정으로 뿌리준위사용자들만이 체계에서 봉사기처럼 동작하는 쏘프트웨어를 쓸수 있다. 이것은 공격자가 임의의 봉사기쏘프트웨어를 교체하자면 먼저 뿌리준위구좌를 파괴하거나 뿌리준위의 약점을 리용해야 한다는것을 의미한다.

체계손상의 기회를 줄이기 위하여서는 이러한 파일준위접근을 유지하여야 한다. 규칙적인 사용자구좌에는 이 파일들에로의 쓰기접근이 허가되지 말아야 한다.

고려하지 않은 선택안

비루스주사쏘프트웨어는 어떠한가? UNIX관련비루스들은 극히 드물다. 이 체계를 규정대로 리용한다면 비루스감염은 거의 일어 나지 않을것이다. 더 큰 관심은 트로이목마와 웜들에 돌려야 한다.

요 약

이 장에서는 비루스와 트로이목마, 웜들사이의 차이점에 대하여 론의하고 이 매개가 어떻게 감염된 체계에 영향을 주는가에 대하여 고찰하였다. 또한 어떤 방지대책이 준비되여 있고 매개의 효과성은 어떤가에 대하여서도 보았다. 또한 혼합된 망환경을 고찰하고 이것을 감염으로부터 막자면 어떻게 하는것이 가장 좋은가에 대하여서도 고찰하였다.

다음장에서는 여벌복사와 재난회복에 대하여 고찰한다. 이것은 파국적인 사태가 발생하는 경우 마지막방어선을 제공한다. 보안의 견지에서는 항상 최악의 경우도 예견하는것이 좋다.

제１２장. 재난방지와 회복

재난방지는 자원의 파괴가 망운영에 영향을 미치지 않도록 하기 위한 예방단계로서 정의된다. 재난방지를 보험과 같이 생각할수 있다. 즉 필요할 경우에는 돈을 투자한다. 그러나 결코 그렇게 되기를 바란것은 아니다.

재난회복은 긴급대책계획에 대한 모든것이다.

최악의 사태가 결코 일어 나지 않는다는것을 담보하였음에도 불구하고 재난이 현실로 될 때도 있다. 이러한 경우에는 무엇을 할것인가 하는 계획을 가지고 있어야 한다. 이러한 계획은 재난의 마지막방어선이다.

제2장에서는 위험분석과 자기의 중요한 자원들을 알아 두는것의 중요성에 대하여 고찰하였다. 또한 그것에 드는 비용에 대하여서도 고찰하였다. 이 장에서는 이러한 자원들을 접근가능하게 하는데서 어떤 선택안들이 준비되여 있는가를 고찰한다.

재난의 류형

재난의 해결책에는 다음의 두가지가 있다.

- 봉사의 유지와 복구
- 오손되거나 지워 진 정보의 보호 또는 복구

매 류형은 자기의 주장을 가지고 있으며 이 두 류형이 다 포함되지 않는 한 재난의 해결책은 완성될수 없다.

실례로 하나의 봉사기에 설치된 두개의 하드구동기가 함께 거울화되였다고 하자. 거울화란 두개의 디스크가 항상 정확히 같은 정보를 가지고 있다는것을 의미한다. 거울화가 쓰이면 하나의 하드구동기의 파괴가 전체 봉사기에 영향을 주지 않는다. 그것은 남은 하드구동기가 계속 파일정보를 보존하며 이전에 기억된 정보에로의 사용자접근을 보장하기때문이다.

거울화는 하나의 재난회복봉사로 볼수 있다. 왜냐하면 그것이 파일봉사를 쓸모 있게 하여 주기때문이다.

사용자가 관리자에게 와서 자기가 3달전에 지워 버린 파일을 회복해 줄것을 요구한다고 하자. 많은 시간이 지나감에도 불구하고 이 정보가 지금 그에게 다시 중요하게 되였으나 그 정보를 다시 만들수는 없었다. 거울화가 파일봉사기에서 유일한 재난회복대책으로 리용되는 경우에 곤난한 문제가 발생한다. 거울화는 파일들이 두 하드구동기에 동시에 기억되여 있다는것을 보증하며 또한 파일들이 지워 지는 경우에 두 디스크에서 동시에 제거된다는것을 보증한다. 거울화를 리용하면 잃어 진 정보를 회복할수 없다.

일러두기

재난회복대책을 세울 때 봉사기고장의 회복과 함께 잃어 진 정보를 회복하는 방법도 고려하여야 한다. 이것들은 둘다 재난위기에 대한 긴급대책에서 중요한 문제로 된다.

망 재 난

망재난은 전체 통신을 중단시킬수 있다. 그러나 망재난에 대하여서는 봉사기들보다 적게 주의가 돌려 지고 있다. 대부분의 기관들은 봉사기를 안전하게 하는데 큰 노력을 기울이고 있다. 이 봉사기들을 련결시켜 주는것이 망임에도 불구하고 망에는 같은 준위의 보안이 보장되지 않고 있다. 망이 동작하지 않는다면 봉사기도 거의 쓸모 없다.

다음절에서는 여러가지 망기술들과 그것에 영향을 줄수 있는 약점들에 대하여 고찰한다. 이것은 많은 정보를 줄수 있지만 이 약점들과 특징들을 구체적으로 리해하게 되면 더 큰 걱정거리가 생긴다(특히 고장을 쉽게 식별할수 없을 때).

매체

재난회복절차는 망매체로부터 시작하여야 한다. 대부분의 국부망들에서는 물리적인 케블을 기본으로 사용하고 있지만 무선매체들이 급속히 보급되고 있는 현재의 환경에서는 매체를 전체적인 재난회복의 한 부분으로 고찰하여야 한다. 사용하는 케블이 망의 고장에 얼마나 견디는가를 결정하는것은 어렵다. 어느 매체를 선택하든지 그것은 전체 망통신을 책임지며 따라서 매체준위에서의 고장은 치명적이다.

가는망과 굵은망

가는망과 굵은망케블은 1970년대에 원래의 이써네트망에서 쓰이였다. 이 두 케블들은 여러개의 체계들이 케블의 같은 론리적인 토막에 접속할수 있게 한다. 케블의 임의의 부분에 고장이 생기면 여기에 련결된 모든 체계는 통신할수 없으므로 이 케블은 고장의 중심점으로 된다.

지난 2년간 100개이상의 회사들중 어느 하나도 가는망케블이나 굵은망케블을 리용하여 새롭게 설치를 하지 않았다.

그런데 유감스럽게도 그들중 15%가 아직도 망의 워크스테이션나 봉사기접근에 가는망케블을 쓰고 있었다. 그리고 2개의 회사가 여전히 굵은망케블을 쓰고 있었다.

일러두기

망의 능력을 높이기 위한 가장 큰 방도의 하나는 가는망케블과 굵은망케블을 새로운 매체로 바꾸는것이다.

꼬임쌍선

류형 5(CAT 5)케블은 대부분의 망설치에 쓰이는 표준케블이다. 지금 대역너비증가요구에 따라 빛섬유케블로 교체되고 있지만 적어도 몇년동안은 CAT 5케블을 쓸것이다.

실례로 기가비트이써네트는 빛섬유케블에 기초하고 있지만 짧은 길이의 케블(50～75m)에 대하여서는 CAT 5케블도 쓸수 있게 되여 있다.

문제는 아직도 류형 3(CAT 3)케블이 많이 쓰이고 있으며 10MB전송용으로 검사된 케블들을 리용할 때 제기된다. CAT 5는 100MB이상의 전송을 담보하지는 못하지만 이러한 속도를 지원할수는 있다. 100MB이상의 고속장치들에서는 CAT 3이나 CAT 5케블을 교체하여야 한다. 이러한 경우에 망에 과부하가 생기지 않는다면 문제는 발생하지 않는다. 물론 과부하는 많은 사용자들이 망봉사에 의거하고 있다는것을 의미한다. 이때 성능이 나쁜 케블을 쓰면 망의 속도를 떨구어 파케트전송을 방해하고 지어 사용자들의 봉사를 단절한다.

이러한 문제의 가장 좋은 해결책은 케블을 쓰기전에 검사하고 확인하는것이다. 만일 이것이 불가능하다면 또는 낮은 등급의 케블을 여전히 리용하여야 한다면 하나이상의 교환기를 리용하여 이 문제를 해결할수 있다. 교환기는 파케트완충능력을 가지고 있으며 여러개의 충돌령역으로 전송을 분리시킨다. 이것이 고장을 다는 극복할수 없으나 케블의 문제가 망에 주는 영향을 어느 정도 감소시킬수 있다.

빛섬유케블

빛섬유케블은 망정보전송에 빛을 쓰기때문에 전자기간섭(EMI)의 영향을 받지 않는다. EMI는 전송오유를 발생시키며 특히 케블이 과부하를 받으면 그 효과가 더 커진다. 빛섬유케블을 선택하는것은 EMI영향을 피하는 좋은 방법으로 되며 빛섬유케블로써 실현되는 봉사들의 믿음성을 높인다.

주　의

빛섬유케블에 대하여서는 제4장에서 구체적으로 고찰하였다.

지나친 케블길이

매 론리적위상구조는 리용할수 있는 최대케블길이를 규정하고 있다. 실례로 10MB 및 100MB이써네트는 꼬임쌍선케블토막의 길이가 100m를 초과하지 못하도록 규정하고 있다. 이러한 규정은 케블의 한끝에 있는 체계가 그것의 다른 끝에 있는 체계의 자료전송을 정확히 검출할수 있도록 한다.

케블길이가 초과되면 낮은 신호세기와 충돌의 증가로 인한 통신속도저하로 하여 고장이 생길수 있다. 이러한 문제들이 일정하지 않는것으로 하여 고장원인을 찾아 내는것이 매우 어렵다.

일러두기

케블길이한계가 초과되는것을 검사하기 위하여 케블검사기를 사용하는것이 좋다.

무선기술들

일부 망들은 무선매체를 리용한다. 무선기술은 현재까지 전송속도가 낮고 공통적인 표준이 부족한것으로 하여 시장점유에서 제한을 받고 있다. 새로운 기술과 표준의 채택으로 하여(특히 802.11b) 고속무선국부망(WLAN)은 현재 널리 보급되고 있다.

WLAN은 위치에 관계없이 동작하는 전송체계로서 망련결에서 케블대신에 라지오파를 리용한다. 기업환경에서 WLAN은 보통 유선망과 의뢰기그룹사이의 련결로 쓰인다.

그러나 무선기술리용에도 여전히 위협이 존재한다.

간섭 802.11b가 무선국부망의 표준으로 제기되였지만 다른 경쟁하는 표준들(HomeRF와 Bluetooth)도 있다. 2001년에 FCC는 HomeRF가 주파수대역을 늘일수 있으며 따라서 802.11b의 대역과 겹칠수 있다고 규정하였다. HomeRF는 가장 좋은 신호를 얻기 위하여(그리고 다른 신호들을 피하기 위하여) 주파수에서 주파수에로 움직이는 주파수도약통신(freguemy-fopping)을 리용하지만 802.11b는 그렇지 못하다. 결과적으로 802.11b규약을 리용하는 국들은 HomeRF를 리용하는 국들과 간섭할수 있다.

설치와 구성 이동할수 있다는 무선망의 우점이 사실상 문제점으로 되고 있다. 이동통신사용자들은 휴대용전화와 마찬가지로 하나의 접근점으로부터 다른 점으로 옮겨 져야 한다. 한 지역을 포괄하는 충분한 접근점들이 부족하거나 그것들이 정확히 구성되지 못하면 망의 통신은 실현될수 없다.

중요한것은 무선기술이 재난회복계획의 좋은 부분으로 될수 있으며 유선망체계가 고장나는 경우에 하나의 여벌체계로 리용될수 있다는것이다. 또한 WLAN들은 점차 현존 유선망에 합쳐 지기때문에 유선망자체가 WLAN의 고장의 경우에 여벌계획으로 된다.

위상구조

망위상구조의 선택은 망이 고장에 얼마나 강한가 하는데 큰 영향을 미친다. 다음절에서 보게 되겠지만 일부 위상구조들은 여러가지 문제들을 회복하는데 좋은 해결책을 준다. 현재 있는 망위상구조를 변화시킬 필요는 없다. 이 절에서는 몇가지 공통적인 문제점들을 지적하고 그것에 따르는 긴급회복계획에 대하여 고찰한다.

이써네트

이써네트는 대부분의 망환경에서 사용하는 위상구조이다. 꼬임쌍선을 쓰는 경우 이 위상구조는 임의의 토막우에서의 케블문제로 하여 제기되는 고장에 강하다. 이것은 체계들을 분리시켜 하나의 체계만이 고장의 영향을 받도록 한다. 물론 이 하나의 체계가 봉사기라면 련결의 단절은 여러 사용자들에게 영향을 줄수 있다.

이써네트망의 가장 큰 약점은 하나의 체계가 모든 유용한 대역너비를 다 차지할수 있다는것이다. 현대의 망카드들에서는 이것이 일반적인 문제로 되지 않지만 이전의 망대면부기판들에서는 여러 체계가 동시에 망전송을 요구하는 문제가 제기되군 하였다. 매 체계는 다른 체계가 전송을 끝내기를 기다리고 있다가 그것이 끝나면 또 전송을 시작한다. 이로 하여 충돌이 많아 지며 망의 성능이 떨어 지게 된다.

기술의 발전과 함께 이 문제는 현재 거의 극복되였다. 교환기는 전체 망환경을 일정한 충돌령역으로 분리시킨다. 이것은 고장이 발생한 체계를 고립시켜 망의 다른 체계의

전송에 영향을 주지 못하게 한다.

통표고리형위상구조

통표고리형은 고장에 견디게 설계되였지만 문제가 없는것은 아니다. 통표고리형은 모든 체계들이 계획적으로 동작할 때 좋은 위상구조로 된다. 실례로 통표고리형망에 접근된 NIC는 그 고리우의 다른 NIC들이 문제가 있다는것을 알리는 경우 자체진단검사를 진행할수 있다. 고장난 NIC는 자체진단검사를 할수 없다. 만일 그 NIC를 정상이라고 본다면 고리에서는 문제가 계속 발생되게 된다.

통표고리형의 하나의 가능한 고장조건은 NIC가 다른 전송속도를 검출하는것이다. 통표고리형은 매 체계가 통표를 다음 체계에 성과적으로 통과시킬것을 요구하기때문에 다른 전송속도로 설정된 하나의 NIC는 전체의 체계에 영향을 줄수 있다. 실례로 고리의 매 체계가 16MB로 설정되였다고 하자. 한 체계가 이 고리에 련결되였는데 4MB로 설정되였다면 모든 통신이 멎어 버릴것이다. 그 리유는 새로운 체계가 통표를 너무 느리게 통과시켜 다른 체계들이 통표가 잃어 진것처럼 생각하게 하기때문이다. 통표가 지나갈 때 고장조건이 명백하지만 부정확하게 구성된 체계에서는 달라 진다. 그것은 그 고리에 대하여 동작상태와 고장상태를 정확히 구별할수 없기때문이다.

통표고리교환기는 다른 전송속도로 설정된 한 체계가 고리망의 나머지 부분에 영향을 주지 않도록 완화한다. 교환기를 리용하면 고리가 16MB로 동작할 때 하나의 체계는 4MB로 동작할수 있다. 그런데 통표고리교환기는 대중적으로 쓰이지 못하며 이써네트의 교환기보다 훨씬 비싸다. 그러므로 이 교환기는 거의 쓰이지 않고 있다.

주 의

이써네트망은 그러한 난점을 가지지 않는다. 하나의 체계가 다른 전송속도로 설정될 때 그 체계만이 영향을 받는다. 다른 모든 체계들은 정상으로 통신을 계속할수 있다.

만일 통표고리형에서 두개의 체계가 같은 매체접근조종(MAC)번호를 가진다면 무슨 일이 일어 나겠는가? 이써네트환경에서 2중MAC는 같은 번호를 리용하는 2개의 체계들에만 영향을 준다. 그런데 통표고리형에서는 2중MAC가 전체 고리를 멈춰 세울수 있다. 그 리유는 통표고리형이 매 체계가 통표를 수신하는 체계와 송신해야 할 체계(자기의 린접체계들)의 MAC주소를 가지고 있을것을 요구하기때문이다. 2중MAC주소는 고리체계를 완전히 혼란시킨다.

빛섬유분산자료대면부(FDDI)

빛섬유분산자료대면부는 고리형위상이지만 통표고리형에서 나타나는 많은 문제점들을 고려하여 두번째 고리를 추가하였다. 이 두번째 고리는 고장이 발견되지 않으면 동작하지 않는다. 고장이 발생하면 FDDI체계가 동작하여 문제가 발생한 령역을 격리시킨다. FDDI는 낡은 기술로 간주되고 있다. 왜냐하면 속도를 100MB이상으로 높일수 없기때문이다. 그러나 이 기술은 고장견딤성이 강한것으로 하여 여전히 리용하고 있다.

주 의

FDDI는 전2중방식으로 동작할수도 있다. 이 경우에 두 고리는 항상 동작상태에 있다. 그러므로 두번째 고리를 예비로 쓸수 없다.

FDDI고리환경에서 그것의 매개 국은 케블이나 장치의 고장을 막기 위하여 두 고리에 다 련결된다. 그림 12-1에서 두개의 경로기사이에 케블고장이 생겼다고 하자. 이 케블고장이 생기면 체계는 더이상 자료를 받을수 없다는것을 재빨리 알아 차린다. 그리고 비콘이라고 하는 특별한 유지파케트를 전송하기 시작한다. 비콘은 고리상의 다른 체계들에 문제가 검출되였다는것을 알리기 위하여 리용한다. 비콘파케트는 다음의 내용을 담고 있다. 《나의 이웃에 문제가 발생하였다고 생각한다. 왜냐하면 내가 더이상 자료를 받지 못하기때문이다.》 다음에 그 국은 두번째 고리우에서 자기의 련결을 초기화하여 접근기 A에서 자료를 주고 받을수 있게 한다.

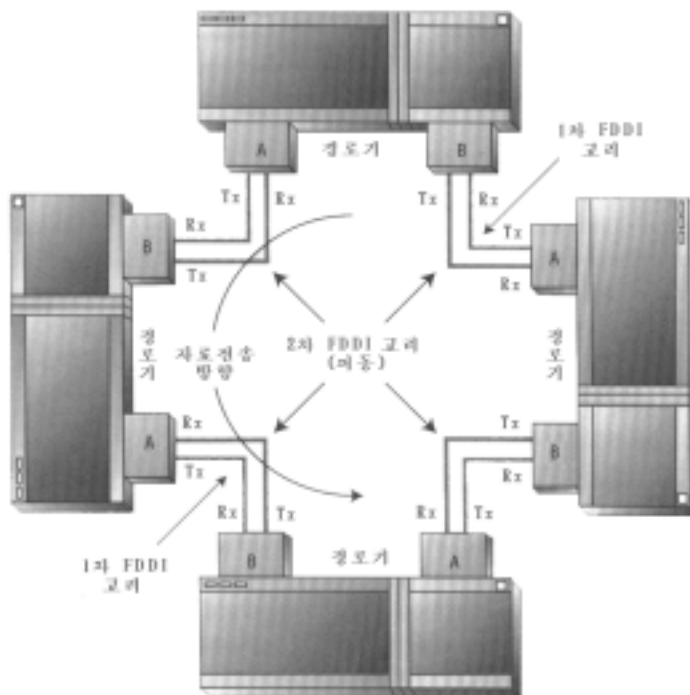



그림 12-1. FDDI고리에 련결된 4개의 경로기

비콘파케트는 그것이 체계의 반대쪽 이웃에 이를 때까지 계속 송신된다. 반대쪽 이웃은 그다음 두번째 고리에로의 련결을 초기화하여 접근기 B우에서 자료를 주고받을수 있게 된다. 이렇게 하여 문제가 발생한 령역을 고립시키고 정상적인 련결에로 돌아 가게 한다. 비콘을 전송하는 국이 자기의 비콘을 받으면 전송을 중지하며 고리의 정상동작으로 들어 간다. 최종 전송경로는 그림 12-2의 망과 류사하다. 비콘파케트를 리용하여 망의 체계들은 고장령역을 결정하고 두번째 고리를 동작시켜 그 령역을 격리시킬수 있다.

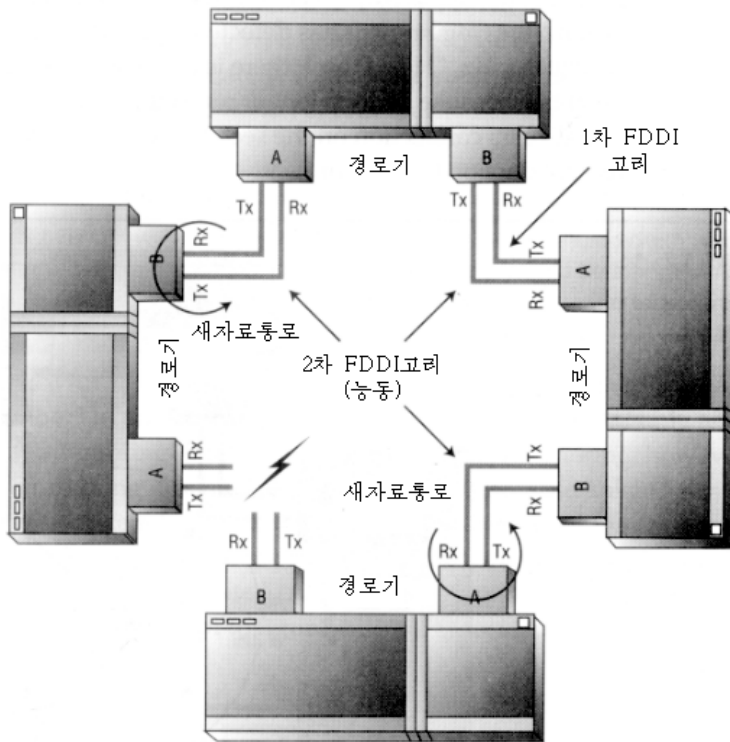



그림 12-2. 케블고장으로부터 회복되는 FDDI국들

만일 이것이 반대쪽 이웃에서 발생한 하드웨어고장이고 그 체계가 두번째 고리를 초기화할수 없다면 하드웨어고장이 생긴 체계의 이웃체계가 그것을 다시 검출하고 문제가 발생한 하드웨어를 격리시킨다. 그러나 망의 나머지 부분은 자기의 기능을 계속 수행한다.

매 경로기는 련결이 회복될 때까지 고장난 부분을 계속 감시한다. 련결이 회복되면 원래의 고리는 완전동작에로 돌아 가며 두번째 고리는 다시 정지한다. 이런 형태의 고장극복성은 련결이 한주에 7일, 하루에 24시간동안 계속 유지되여야 하는 환경(24×7동작이라고 한다.)에서 매우 중요한것이다. 이 기능으로 하여 FDDI가 오늘날 국부망들중에서 가장 고장에 잘 견디는 망위상구조로 되였다.

주 의

FDDI는 별형위상구조를 지원할수도 있다. 이것은 여분을 제공하지 않는다. FDDI망은 별형구조와 고리형구조로 구성될수 있다.

802.11b(WLAN)

802.11b표준은 두개의 기본요소들을 정의한다.

국 보통 이것은 무선NIC를 가진 PC이다.

접근점 접근점(AP)은 유선망과 무선콤퓨터사이의 다리로써 동작한다. 접근점은 무선 및 유선대면부(이써네트)와 다리기능쏘프트웨어로 구성되는데

하나 또는 여러개의 국들이 망에 련결되도록 하는 기초이다.

802.11b는 또한 두가지 방식으로 동작한다.

기반구조 이 방식은 기초봉사모임(BSS)이라고도 하는데 유선망에 련결된 적어도 하나의 접근점과 하나 또는 여러개의 무선국집단에 련결된 하나의 접근점을 가지는 무선망이다. 하나의 부분망에 있는 두개 또는 그이상의 BSS들을 확장봉사모임(ESS)이라고 부른다. 기반구조방식은 기업환경에서 가장 일반적인 방식이다.

림시방식 이 방식을 독립BSS(IBSS) 또는 동등방식이라고도 한다. AP의 다리봉사들이 없이 직접 통신하는 무선국들의 집단으로 이루어 져 있다.

이써네트(802.3)와 마찬가지로 802.11b는 송신전에 송신자가 매체를 감시하도록 한다. 이써네트에서 완전접근규약은 반송파수감다중접근/충돌검출(CSMA/CA)로 알려 져 있다. 무선망에서는 충돌검사가 가능하지 않다. 왜냐하면 하나의 국이 동시에 송신과 듣기를 할수 없으며 따라서 충돌이 발생한다는것을 알수 없기때문이다.

이것을 보상하기 위하여 802.11b는 반송파수감다중접근/충돌회피(CSMA/CA)라고 하는 수정판을 리용한다. CSMA/CA는 다음과 같이 동작한다. 송신자는 듣고 있다가 이무런 행동도 나타나지 않으면 추가적인 우연시간동안 기다리다가 전송한다. 파케트를 완전히 받으면 수신자는 송신자에게 응답을 보내여 그 과정을 완료한다. 응답이 수신되지 않으면 충돌이라고 가정하고 그 파케트를 재전송한다. 유감스럽게도 CSMA/CA에는 추가적인 처리가 포함되므로 등가인 이써네트망보다 속도가 느리다.

또 다른 가능한 문제는 《숨겨 진 마디》라고 하는데 여기서 접근점의 반대쪽에 있는 두 국은 접근점으로부터의 활동은 들을수 있지만 서로는 듣지 못한다. 다행히도 802.11b에는 전송요청/전송지우기(RTS/CTS)라는 선택안을 가지고 있다. 이 규약은 송신자가 먼저 RTS를 송신하고 그다음 AP에서의 CTS를 기다리게 한다. 모든 국들이 AP를 들을수 있기때문에 CTS를 기다리는것은 송신은 느리지만 매 송신자가 충돌없이 통신하게 한다. 그러나 RTS/CTS는 부차적인 처리를 가지고 있으며 이것은 또 하나의 잠재적인 결점으로 된다.

여러개의 AP를 가진 WLAN을 설계하여 단일고장점을 피할수 있다. 국이 자기의 원래 AP로부터 물리적으로 멀어 지는것으로 하여 새로운 AP와의 재결합이 발생하지만 이것은 무선특성의 변환 또는 큰 망자료흐름에 의하여서도 발생할수 있으며 이로 하여 부하균형을 실현할수 있다.

임대선 또는 T1련결

임대선 또는 T1 련결과 같은 전용회선WAN위상구조들은 내부비밀을 담보하는 좋은 방법이기는 하나 단일고장점문제가 제기된다. 임대선이나 T1련결은 두개의 멀리 떨어 져 있는 싸이트들사이의 하나의 긴 케블과 등가이다. 만일 이 회선의 일부가 차단되면 이 두개의 싸이트들사이에 정보가 여전히 교환된다는것을 담보하는 여유가 없

게 된다.

전용회선을 리용할 때 이 절의 뒤에서 취급하는 상사 또는 ISDN여유선택안을 고려하여야 한다. 만일 봉사기들을 현장사무소로부터 중심위치에로 옮기는 최근의 추세에 따르고 있다면 이것은 특별히 중요하다. 이것은 하나의 관리점을 제공하지만 또한 단일고장점도 만든다. 봉사기가 없는 현장사무소가 기본사무소와의 전용회선련결을 잃으면 이 현장사무소에는 망자원들을 잃게 된다. 만일 회사가 약한 의뢰기구조를 리용하였다면 이 현장사무소는 완전히 페쇄될것이다.

프레임중계

프레임중계도 WAN의 련결을 제공할수 있지만 그것은 공유된 공공망을 통하여 제공된다. 이 망은 만일 프레임중계망의 어떤 토막이 고장난다면 자료흐름은 임의의 련결을 통하여 전달될수 있다는 의미에서 파케트교환망이다. 이것은 약간의 자료흐름혼잡을 일으킬수 있지만 적어도 련결성은 보장한다.

그러나 전체 프레임중계망이 정지되는것이 불가능하지는 않다. 이러한 사건이 최근에 MCI와 AT&T에서 발생하였다. 이 두 경우에 모든 리용이 중단되였다. 이것은 의뢰기의 위치에 따라서 몇시간으로부터 며칠까지 지속되였다. 이러한 정지상태들은 드물지만 이 고장들이 발생할수 있다는것을 고려하여야 한다.

일러두기

프레임중계망이 전용회선들보다 더 좋은 고장견딤성을 제공하고 있지만 고장에 안전하지는 않다. WAN토막이 하루 24시간 한주 7일(24×7)동안 계속 동작하는 프레임중계망우에서 동작한다면 회선에 대한 어떤 여유를 설정하는것을 고려하여야 한다.

수자식종합통신망(ISDN)

ISDN은 64Kbps이상의 수자식봉사를 제공하는 전화회사기술이다. ISDN은 1980년대 초기부터 쓰이였지만 상사모뎀의 제한과 새로운 파케트교환기술의 도입에 의하여 1990년대 후반기에야 광범히 실현되였다. ISDN은 전화교환기들에 수자식교환련결을 지원하는 봉사설치를 요구한다. ISDN은 초기에 설치비용이 비싸고 표준들의 결핍 그리고 적은 수의 사용자 등의 문제들을 가지고 있었다.

ISDN련결에 포함된 회선들은 전용으로 주어 지기때문에 하나의 회선차단은 전체 련결의 고장으로 이어 진다. 어떤 회사에 대하여서는 이것이 괜찮은 선택안이고 또 어떤 지역에서는 값 눅은 인터네트접근만이 유일한 선택이지만 가장 현대적인 회사들은 DSL이 비록 자기의 실현문제로 하여 다소 복잡하지만 DSL기술은 값 눅고 유연성이 있다. 여전히 ISDN은 그것의 안전한 성능과 고장력사가 없는것으로 하여 잘 알려 진 기술로 남아 있다.

수자식가입자선

수자식가입자선(DSL)은 현존의 동선을 리용하고 중심교환기까지의 짧은 거리(l8000ft이하)를 요구한다는 면에서 ISDN과 비슷하다. DSL은 회선지향이지만 전체 길이의 련결에 대하여 고정된 물리적회선을 리용하는것이 아니라 LECs POP에로의 완전한 회선을 요구한다. 이것은 임의의 주어 진 련결에서 고장점들의 수를 줄인다. DSL은 또한 ISDN보다 더 높은 준위의 속도 즉 52Mbps까지의 내리흐름속도와 lMbps까지의 올리흐름속도를 제공한다. 이 속도는 ISDN 또는 T1에서와 같이 고정되는것이 아니며 이것은 비데오회의나 다른 다매체리용들에서는 련결의 두 방향과 관련하여 문제를 초래할수 있다.

단일고장점

앞절에서도 짐작할수 있는바와 같이 망우에서 재난을 줄이는 가장 좋은 방법은 단일고장점들을 확인하고 여유를 설정하거나 긴급대책계획을 세우는것이다. 모르고 단일고장점을 만드는것은 망설계에서 생기는 가장 일반적인 오유이다.

실례로 보통의 인테네트련결의 구성을 고찰하자.

- 단일방화벽
- 단일경로기
- 단일CPU/DSU
- 단일임대선이나 T1련결

이 구성은 3개의 전자장치와 인터네트련결을 모두 중단시킬수 있는 통제밖에 있는 망회선을 가지고 있다. 이 장치들은 쉽게 교체할수 있는 요소들이 아니다. WAN회선는 국부교환회사에 의하여 조종되며 따라서 응답시간은 국부교환회사와 가지게 되는 기업상관계의 직접적인 영향을 받는다. 일부 기관들에서는 이런 문제를 크게 보지 않으나 많은 기관들은 자기의 매일 사업의 한 부분으로서 인터네트련결에 의거한다. 인터네트련결이 처음 리용될 때 인터네트봉사에로의 접근은 중요한 문제로 간주되지 않는다.

지금 인터네트접근은 중요한 기업기능으로 되였으므로 누구도 인터네트봉사를 잃는다는데 대하여서는 생각하지 않다. 따라서 위험분석에로 되돌아 가서 망의 단일고장점을 확인하여야 한다. 또한 봉사를 잃는것이 주는 영향을 평가하여야 한다. 만일 망의 어떤 점이 중요하다고 보아 지면 여분을 구축하여야 한다.

설비보강

1990년대 초에 집선기는 높은 포구밀도과 단일고장점으로 하여 많이 대중화되였다. 하나의 집선기를 통하여 200개이상의 체계들을 련결하는것이 보통 현상으로 되였다. 물론 망토막에 200이상의 사용자들을 련결하는것은 전원문제나 관리 등의 문제로 하여 곤난하다. 그러므로 많은 기관들은 여러개의 집선기들을 리용하려고 하고 있다. 설치공간은 더 필요하지만 하나의 집선기의 고장이 전체 망에 영향을 주지 않는다.

Cisco, Cabletron등의 회사들로부터 이러한 제품들이 제공된다. 이전의 집선기와 마찬가지로 이 제품들은 중앙관리점에 의하여 관리비용을 낮춘다고 주장한다. 이 주장도

일리는 있지만 이것은 하나의 장치의 파국적인 고장에 의한 재정적인 손실에 대하여서는 말하지 않고 있다.

장치의 다중리용은 고장의 회복에서 보다 많은 유연성을 보장한다. 실례로 하나의 교환기대신에 6개의 교환기를 리용하면 하나가 고장난다고 하여도 망동작이 정지되지는 않는다. 고장난 장치가 있다고 하여도 얼마간의 여유는 가지게 될것이다. 나머지 5개의 장치들을 리용하여 중요한 사용자들에 대한 봉사를 계속할수 있다.

여분의 LAN경로의 우점

제3장에서 본바와 같이 강한 동적경로조종을 리용하면 망토막들사이에 여러개의 경로들을 얻을수 있다. 일부 경로조종규약들은 어느 경로가 가장 좋은 경로인가를 결정하는 척도로서 망리용률과 같은것을 고려하고 있다.

정적경로들은 하나의 경로만이 있을 때(WAN련결과 같은) 또는 공격자가 경로표를 혼란시킬수 있는(인터네트련결과 같은) 지역에서는 좋을수 있지만 내부망에 대하여서는 OSPF와 같은 동적경로조종을 리용하여야 한다. 매 토막들사이에 하나의 련결점만이 있다면 다른 경로기를 예비로 구입하거나 자기봉사기들에 망기판추가를 고려하여야 한다. 도약수와 비용과 같은 척도들을 리용하면 망을 긴급사태의 경우에 봉사기를 통하여 경로조종하도록 구성할수 있다. 이것은 원래의 경로기가 고장나지 않는 한 봉사기에 추가적인 부하가 걸리지 않는다는것을 담보할수 있게 한다.

WAN련결을 위한 전화선여벌

WAN련결은 단일고장점을 제공하는 중요한 후보로 된다. WAN련결을 유지하는 비용으로 하여 대부분의 회사들은 자기의 WAN에로의 어떤 형태의 여유를 설정하지 않는다. 그렇게 되면 망의 이 부분에 대한 실제적인 조종을 할수 없게 된다. 고장과 관련한 망문제를 해결하는것은 모두 통신회사의 처분에 달려 있다.

한가지 가능한 해결책은 경계선경로기들이 만일 원래의 선이 고장나는 경우에 여벌회선으로 넘어 가도록 구성하는것이다. 이 여벌회선은 한쌍의 모뎀에 따르는 상사식전화선으로 될수 있으며 또는 ISDN을 리용하여 대역너비를 늘인것일수도 있다. 이때 선이 T1이라면 대역너비는 작아 지지만 두 위치사이에 대역너비가 전혀 없는것보다는 낫다.

경로기가 전화선여유를 가지도록 구성하는것은 어렵지 않다. 다음의 실례는 serial 0우의 원래의 회선이 응답에서 실패하였을 때 Cisco경로기가 bri 0우의 ISDN의 련결을 실현하도록 요구하는 명령들을 보여 주고 있다.

```
interface serial 0
여벌복사 delay 10 120
여벌복사 interface bri 0
ip address 192.168.5.1 255.255.255.0
!
interface bri 0
ip address 192.168.5.2 255.255.255.0
```

```
dialer string 5551212
dialer-group 1
dialer in-band
dialer string 5551212
async dynamic routing
!
dialer-list 1 protocol ip permit
```

이 구성은 만일 serial 0이 10s동안 응답하지 않으면 bri 0대면부가 예비경로로 기동된다는것을 경로기에 알리고 있다. 마찬가지로 만일 serial 0회선이 최소 120s동안 동작상태로 돌아 오면 bri 0선은 다시 취소되여야 한다. dialer-list명령은 또 하나의 회선경로를 가져 올수 있는 자료흐름의 형태를 확인한다. 이 경우에는 임의의 IP자료흐름이 그 회선을 기동시킬수 있다고 규정하였다.

일러두기

만일 여벌해결을 위하여 ISDN을 리용한다면 또는 여러개의 현장사무실련결을 BRI로 접수하기 위하여 기본사무실에서 PRI를 리용한다면 호출이 회선의 BRI측으로부터 개시된다는것을 기억하여야 한다.

구성파일들의 보관

지금까지 론의한 망재난의 해결책들은 모두 봉사의 유용성에 대하여 취급하였다. 이 장의 앞에서 언급한바와 같이 잃어 버린 정보를 다시 회복할수 없는 한 재난회복은 완성될수 없다. 이 경우 망을 따라 흐르는 자료에 대하여는 문제가 되지 않는다. 규약들은 이 정보가 없어 지지 않았다는것을 확인할수 있게 해준다. 실제로 관심하여야 할것은 경로기나 교환기 그리고 집선기들을 프로그람화하는데 리용되는 구성파일들이다.

망장치가 고장나면 그안에 프로그람화된 구성정보를 잃을것이다. 어떤 사람들은 구성정보를 리용할수 없는 상태로 변화시킬수도 있다. 만일 이러한 경우가 발생하면 구성파일의 여벌복사를 가지고 있다가 원래의 설정을 회복하는것이 좋다. 이것은 또한 망에 언제 어떤 변화가 생겼는가를 알려고 할 때 효과적이다.

말단경과기록

자기의 구성정보를 보관하는 가장 쉬운 방법은 말단경과기록이다. 대부분의 말단모방 및 telnet프로그람들은 말단화면으로 흐르는 모든 정보들을 기록하는 방법들을 가지고 있다. 망장치가 모든 구성정보를 보여 주는 단일지령을 가지고 있다면 이 정보를 후에 재생하기 위하여 말단경과기록을 리용할수 있다.

Cisco경로기나 교환기와 같은 일부 장치들은 그 장치를 구성하기 위하여 이 정보를 말단화면에 보여 주게 한다. 실례로 write term지령은 모든 구성정보를 말단화면에 표시

한다. 이것은 이 구성정보가 쉽게 기억되도록 한다. 만일 장치가 후에 고장나면 새로운 장치로 말단대화를 열고 구성방식에 넣는다. 원래 장치의 원래구성을 오려둠판에 복사하고(Notepad나 Wordpad를 리용하여) 그것을 새 장치에 련결된 말단화면에 붙여야 한다. 그 구성정보를 보관하면 새로운 장치가 준비된것으로 된다.

말단경과기록의 약점은 그것이 구성을 위하여서만 동작한다는것이다. 조작체계를 기억시킬수는 없다. 또한 망장치가 모든 구성정보를 표시하는 단일지령을 제공하지 않으면 구성을 기록하는 과정은 길어 질수 있다.

TFTP봉사기

TFTP는 FTP와 류사한데 전송층규약으로서 UDP를 리용하며 어떠한 형태의 인증도 리용하지 않는다. 의뢰기가 파일을 TFTP봉사기로부터 검색하거나 파일을 TFTP봉사기에 보관할 때 파일의 이름과 TFTP봉사기의 IP주소만 알면 된다. 인증하거나 새로운 등록부를 변화시키도록 하는 지령파라메터들은 없다.

TFTP는 인증이 없으므로 방화벽을 리용할 때 문제가 생길수 있다. 그러나 대부분의 망장치들은 구성정보를 보관하거나 회복하기 위하여 TFTP를 지원한다. 하나의 TFTP봉사기는 망우의 매 장치에 대한 구성파일들은 기록할수 있다. 만일 망우의 한 장치가 고장난다면 간단히 그것을 접속하고 IP주소를 할당하며 TFTP를 리용하여 요구되는 구성파일을 복구할수 있다.

일러두기

대부분의 제작자들은 최신의 조작체계를 가지고 장치를 구성하기 위하여 TFTP를 리용한다. 이것은 요구되는 구성을 가지고 TFTP봉사기우에서 안정한 조작체계를 유지할수 있다는것을 의미한다. 장치를 교체할 때 TFTP를 리용하여 TFTP봉사기로부터 조작체계와 구성파일을 적재한다.

망장치로부터 구성정보를 보관함으로써 망재난으로부터 될수록 빨리 회복할수 있다.

봉사기재난

앞에서는 어떻게 하면 망이 고장에 더 잘 견디도록 할수 있겠는가에 대하여 보았다. 여기서는 봉사기에 관한 문제들을 고찰하기로 한다. 봉사기가 재난에 견디도록 하는데는 여러가지의 준비된 선택안들이 있다. 제한인자는 비용문제이며 또한 어떤 경우에는 해결책들이 모든 플래트홈에서 다 쓸수 있다고 볼수는 없으므로 조작체계도 문제로 된다. 봉사기재난방지는 보통 비용이 많은 드는것으로 알려 져 있으며 여기서는 단일체계에서의 비용에 대하여서만 고찰할수 있다.

무정전전원(UPS)

모든 콤퓨터들이 깨끗하고 안정한 전원을 요구하지만 특히 콤퓨터가 봉사기로 쓰일 때에는 더욱 중요하다. 왜냐하면 많은 사용자들이 봉사기에 의존하기때문이다. 좋은 전원이란 정전되지 않는 전원이 아니라 전압요동과 급격한 변화에 영향 받지 않는것을 말한다. 10%만한 전원요동이 콤퓨터에서 오유조건으로 된다.

낮은 전압이나 정전은 체계가 재기동하기때문에 쉽게 포착할수 있으나 요동이나 급격한 변화 그리고 잡음 등은 응용프로그람의 오유와 같은 미묘한 문제들을 일으킬수 있다.

전원문제에 대한 추적

한 경험자는 한 의뢰자의 NetWare봉사기에서의 여벌복사프로그람과 관련한 한가지 문제를 해결한적이 있었다. 처음에는 여벌복사프로그람이 CPU를 100% 리용하기때문에 그 봉사기가 기능을 못하는것처럼 보였다. 그런데 이 문제는 여벌복사과정의 우연적인 단계에서 일어 나군 하였다. 이상한것은 의뢰자가 매일 밤 여벌복사프로그람을 돌렸지만 문제는 월요일과 목요일 7시 30분부터 8시사이에만 발생하군 하였다.

사업시간에는 이 문제가 발생하지 않았다. 모든 수정프로그람을 설치하여도 효과가 없었다.

한 경험자는 이 문제를 알아 보기 위하여 목요일밤에 늦게까지 거기에 있었다. 7시에 청소부가 나타나서 휴지통을 버리고 주단을 흡진기로 청소하기 시작하였다. 7시 40분경에 청소부가 그 방의 밖에 있는 전원접속구에 흡진기전원을 넣었다.

흡진기의 전원을 뽑자마자 문제가 발생하였다. 흡진기를 뽑을 때 생긴 전원충격에 의하여 즉시 봉사기의 CPU가 비정상상태로 되였다. 경험자가 청소부에게 매일 밤 흡진기로 청소하는가고 물었더니 그는 월요일과 목요일에만 흡진기로 청소한다고 대답하였다. 결국 그 의뢰자는 다음날에 무정전전원을 구입하였고 문제는 해결되였다

일러두기

좋은 무정전전원은 콤퓨터체계에서도 필요하지만 봉사기에 대하여서는 필수적인 설비로 간주되여야 한다. 지능적인 무정전전원은 전원이 일정한 시간동안 비정상이면 그 봉사기의 전원을 차단하는 프로그람을 가지고 있다. 또한 무정전전원을 쓰면 축전지전원이 다 방전하여도 봉사기가 고장나지 않도록 할수 있다.

저가격디스크묶음(RAID)

RAID 또는 예비디스크묶음은 하드디스크파괴에 대한 고장견딤성을 제공할뿐아니라 체계성능도 개선할수 있다. RAID는 자료를 여러개의 하드디스크들에 보관한다. 또한 여

러개의 디스크가 큰 파일을 보관하기 위하여 동시에 함께 동작할수 있으므로 성능이 개선된다.

리용하고 있는 RAID의 준위에 따라 체계는 오유정정부호(ECC)라고 하는 기우성정보도 보관할수 있다. 어떤 RAID체계들은 동작중에 교체가능하다. 이것은 콤퓨터가 리용되는 상태에서 구동기를 교체하므로 정지시간이 0이다.

RAID는 하드웨어 또는 쏘프트웨어로 실현될수 있다. 하드웨어RAID에서 RAID는 조작체계에 하나의 론리디스크처럼 보인다. 쏘프트웨어RAID는 현존조작체계의 부분이거나 또는 추가쏘프트웨어의 프로그람코드이다. 쏘프트웨어RAID는 보통 하드웨어RAID보다 느리다. RAID는 RAID 0～RAID 5의 준위로 되여 있다.

주 의

RAID 6～RAID 10도 있으나 이것은 원래의 6개 종류의 단순한 변종들이다.

RAID 0

RAID 0은 정확히 말하여 성능상의 리득을 위하여 사용되며 고장견딤성은 제공하지 않는다. RAID 0은 파일을 하나의 디스크에 보관하는것이 아니라 여러개의 하드디스크들에 나누어서 보관한다. 이것은 구동기들이 기억부하를 공유하게 하여 성능을 개선하지만 하나의 디스크파괴가 전체 묶음에 영향을 주므로 고장기회는 증가한것으로 된다. 이와 같이 고장견딤성이 약한것으로 하여 RAID 0은 널리 쓰이지 않는다.

RAID 1

RAID 1은 매 디스크에 모든 파일정보의 완전한 복사본을 가지고 있다. 이로하여 RAID 1은 디스크거울이라고도 한다. 하나의 디스크가 고장난다고 하여도 나머지 매 디스크들은 전체 파일체계의 모든 복사본을 가진다. 이것은 임의의 한 디스크의 고장에 의한 체계파괴를 막는다. 이것은 또한 체계용량이 단일 디스크의 크기로 제한된다는것을 의미한다. 다시 말하면 꼭같이 거울화된 2개의 4GB구동기들이 있다면 8GB가 아니라 4GB만을 쓸수 있다.

RAID 1디스크묶음은 사실상 하나의 디스크보다 더 잘 동작한다고 볼수 없다. 그것은 디스크조종기가 매개 구동기에 매 파일의 완전한 복사를 보내야 하기때문이다. 이렇게 하면 속도는 가장 느린 디스크보다도 더 느리게 된다. Novell은 디스크거울화의 한가지 변종으로서 디스크중복이라는 기술을 개발하였다. 디스크중복은 디스크거울화와 같은 방법으로 동작하지만 여러개의 조종기카드들을 리용한다. 이렇게 하면 매개 조종기가 하나의 구동기와만 통신하면 되므로 성능이 떨어 지는것을 막을수 있다. 디스크중복은 체계가 구동기고장뿐아니라 조종기고장에도 견딜수 있으므로 고장견딤성도 증가시키는것으로 된다.

RAID 2

RAID 2는 RAID 5와 류사한데 자료는 한번에 한바이트씩 디스크에 보관된다. 또한 하나의 구동기고장이 묶음전체의 고장으로 이어 지는것을 막기 위하여 오유수정이 리용

된다. 다른 RAID묶음들에서 사용되는 블로크방식자료전송은 RAID 2에서 쓰이는 바이트방식보다 훨씬 효과적이다. 이것은 RAID 2는 여러개의 작은 파일들을 취급할 때 성능이 나쁘다. 그러므로 RAID 2는 널리 쓰이지 않는다.

RAID 3과 RAID 4

RAID 3과 RAID 4는 RAID 3이 3개의 디스크를 리용하고 RAID 4가 4개의 디스크를 리용한다는것을 제외하고는 같다. 이 RAID들은 오유정정에 하나의 디스크를 리용하며 나머지 디스크들에는 자료를 나누어 보관한다. 다시 말하여 RAID 4묶음에서 디스크 1~3은 나누어 진 자료들을 포함하며 디스크 4는 오유정정에 쓰인다. 이것은 묶음이 하나의 디스크를 잃는것으로 된다.

ECC는 본질에 있어서 모든 다른 하드구동기들에 보관되여 있는 자료의 수학적인 더하기이다. 이 ECC값은 매 블로크단위로 계산된다. 실례로 다음의 수학문제를 고찰해보자.

$$3 + 4 + 2 + 6 = 15$$

식의 왼변의 모든 값들은 RAID 4묶음의 매 자료디스크우의 특정의 블로크에 기억된 자료를 표시한다. 기우성구동기의 같은 블로크에는 그 합이 보관된다. 이제 디스크 3이 파괴되고 이 블로크집단에 하나의 파일요청이 발생하였다고 하자. RAID묶음에는 다음과 같은 문제가 제기된다.

$$3 + 4 + ? + 6 = 15$$

알수 있는바와 같이 모르는 값을 쉽게 구할수 있다.

이것은 얼마간의 처리를 요구하며 따라서 디스크접근을 좀 느리게 하지만 묶음은 잃어 버린 자료를 재생하며 파일정보를 복귀한다. 이 실례는 매우 단순하지만 RAID 3~5가 어떻게 디스크고장를 회복하는가를 명백히 보여 준다.

하나의 디스크를 리용하는것에 대한 실례를 보기로 하자. 여기서는 고장견딤성을 제공하는데 보다 적은 기억을 리용한다. 자료는 하나의 디스크를 제외한 전체 디스크에 보관되므로 RAID 3 또는 RAID 4묶음의 전체 기억용량은 전체 디스크에서 하나의 디스크용량을 뺀것과 같다. 다시 말하여 RAID 4구성에서 4개의 4GB구동기들을 가진다면 쓸수 있는 용량은 12GB이다.

RAID 5

RAID 5는 RAID 3과 RAID 4와 비슷하나 모든 디스크들이 다 자료와 ECC보관에 리용된다. 이것은 기우성구동기에서 병목문제를 가지는 RAID 3이나 RAID 4보다 속도를 개선한다. 또한 RAID 5를 통하여서는 5개이상의 구동기들을 리용할수 있으므로 기억용량문제도 개선된다. RAID 3이나 RAID 4와 같이 전체 기억용량은 모든 디스크들의 기억용량에서 하나의 디스크의 기억용량을 던것과 같다. RAID 5는 지금까지 디스크거울화후에 가장 널리 쓰이는 RAID묶음이다.

여유봉사기

봉사기여유는 RAID의 개념을 전체 콤퓨터에 적용한다. 이것을 때로 봉사기고장견딤성이라고도 하는데 원래의 하나가 파괴되는 경우에 쓸수 있는 하나 또는 몇개의 체계들을 제공한다. 이것은 고장이 구동기고장이나 기억기고장 또는 지어 모판고장이라고 해도 문제로 되지 않는다. 원래의 봉사기가 요청에 대한 응답을 중지하면 여분체계가 넘겨 받는다.

그림 12-3에서 보여 준바와 같이 여분봉사기들은 보통 2대의 통신통로들을 공유하고 있다. 하나는 봉사기들의 망련결이고 하나는 두 체계사이의 고속련결이다. 실현에 따라 이 련결은 전용통신기판이나 또는 100MB이써네트기판을 리용하여 실현될수 있다. 갱신내용은 고속련결을 통하여 2차봉사기에 조종된다. 실현에 따라 이 갱신내용은 디스크정보로 될수도 있고 기억기주소정보를 포함할수도 있다.

주 의

기억기주소정보가 포함되면 2차봉사기는 봉사를 중단시킴이 없이 1차봉사기로 전환될수 있다.

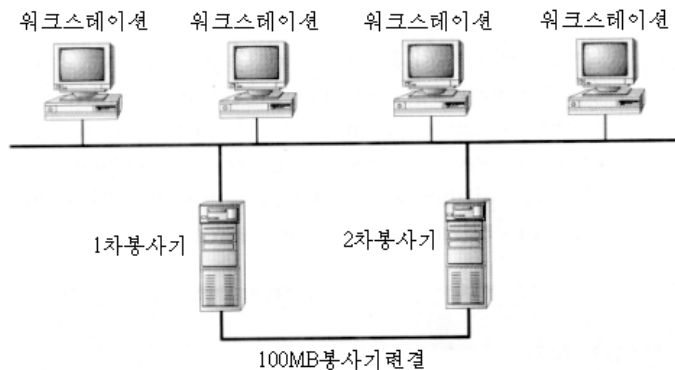



그림 12-3. 여벌봉사기구성

모든 여벌봉사기들이 다 고속련결을 포함하고 있는것은 아니다. 실례로 이 장의 마감에서 보게 되는 Octopus는 정보를 교환할 때 봉사기의 망련결을 리용한다. Octopus는 두 체계들사이의 고속련결을 요구하지 않는다. 현존 망을 리용하는 우점은 2차봉사기가 아무곳이나 지어 원격설비에도 위치할수 있다는것이다. 2차봉사기가 먼 곳의 다른 위치에 안전하게 있을수 있으므로 그것의 설치는 화재나 번개, 폭풍과 같은 설비관련고장문제들에 대하여 매우 견딤성이 높다.

만일 두 체계사이에 련결이 없다면 기억기정보는 공유되지 않으며 2차봉사기는 1차봉사기를 즉시에 교대할수 없다. 1차봉사기에 이미 전송된 의뢰기요청은 시간초과되며 2차봉사기의 봉사를 받기전에 재설정된다. 이것은 2차봉사기가 쓰이기전에 1min 혹은 2min의 지연을 가져 온다. 또 다른 결함은 망의 리용률이 증가된것이다. 이것은 모든 정보가 두 체계사이의 개별적인 련결이 아니라 망을 통하여 공유되기때문이다.

봉사기여유는 조작체계준위에서 또는 추가제품으로 실현될수 있다. Novell의 SFT-Ⅲ과 Microsoft Cluster Server(MSCS)는 조작체계준위에서 여벌봉사기들을 지원하는 좋은 실례로 된다. 여벌봉사기지원을 추가할수 있는 Vinca, Network Integrity, Qualix Group와 같은 회사들의 제품들도 많다. 무엇을 선택하는가 하는것은 요구에 의존할것이다. 매 제품들은 조금씩 차이나는 형태로 여벌봉사기들을 지원한다.

클라스터화

클라스터화는 여벌봉사기와 류사한데 여기서는 모든 체계들이 봉사요청을 처리하는데 참가한다. 클라스터(cluster)는 통신량부하균형을 맞추기 위한 지능단위로 동작한다. 의뢰기의 관점에서 보면 클라스터는 하나의 매우 빠른 봉사기로 볼수 있다. 봉사기가 고장나면 처리는 계속되지만 그 성능은 떨어 진다. 클라스터화가 봉사기여분보다 더 매혹적인 리유는 2차체계가 실제적으로 처리에 참가한다는데 있다. 그것들은 다른 하나의 체계가 고장날 때까지 기다리지 않는다. 이것은 하드웨어의 리용률을 크게 높일수 있게 한다.

Linux클라스터화

클라스터화의 한가지 좋은 실례는 NASA의 Goddard우주비행쎈터(GSFC)의 Beowulf계획이다. 1994년에 NASA의 우주정보과학쎈터(CESDIS)는 16개의 Linux체계를 함께 클라스터화되게 하였다. 모든 체계는 Intel의 486DX4 100MHz 소편에 기초하고 있었으며 클라스터의 전체 가격은 5만딸라이하였다. 클라스터화된 체계들사이의 통신은 하나의 100MB이써네트망을 리용하였다. 목적은 우주과학연구에 쓰이고 있는 높은 급의 워크스테이션기능을 값 눅게 실현하는것이였다.

결과적인 클라스터는 초당 1.2기가의 류동소수점연산(Gigaflop)의 처리속도와 원래체계의 8배인 디스크입출구대역너비를 가지였다. 이 Linux클라스터는 그것보다 4~5배 비싼 대형콤퓨터와 류사한 성능을 가진다.

클라스터화는 고장견딤성과 성능을 다같이 높이는 우수한 방법이며 UNIX와 VMS, Microsoft NT와 2000에서 쓸수 있다.

자료의 여벌복사

자료의 2중복사는 항상 재난이나 손상, 손실을 막는 가장 좋은 방법이다. 전통적인 방법은 테프에 의거하지만 새로운 여벌복사방법들은 인터네트에 기초하고 있으며 외부싸이트에로의 보관을 제공한다.

테프여벌복사

대부분 망관리자들의 주요수단인 테프여벌복사는 손실, 손상되였거나 또는 지워 진 정보들을 보호 및 회복하기 위한 방법이다. 지금까지 고찰한 봉사기에 기초하고 있는 방법들은 모두 봉사기를 하나의 봉사로서 유지 또는 회복하는데 기본을 두고 있다. 그러나 3개월전에 지워 진 파일을 회복할수 있는 방법은 없다. 그러므로 테프가 여벌복사로써 리용되게 된다. 그것의 우점은 봉사기에 보관된 정보들을 안전하게 지키는데 있다.

주 의

파일을 회복하는 능력은 UNIX나 Windows NT를 파일봉사기로 리용할 때 훨씬 더 중요하다. 이러한 조작체계들은 지워 진 망파일들을 회복하는 기능을 가지고 있지 못하다.

대부분의 여벌복사쏘프트웨어는 어느 파일을 테프에 기록하여야 하는가를 선택하기 위한 3가지 방법을 지원한다. 이 방법들은 다음과 같다.

- 완전여벌복사
- 증분식여벌복사
- 차분식여벌복사

완전여벌복사

완전여벌복사는 이름그대로 봉사기의 모든 파일을 다 기록한다. 완전여벌복사는 재난회복에 가장 좋은 방법이다. 그것은 전체 파일체계의 완전한 복사를 하나 또는 여러개의 테프에 보관한다. 완전여벌복사를 수행하는데서 문제는 다른 방법들에 비하여 시간이 오래 걸리는것이다. 많은 량의 정보(실례로 10GB이상)를 여벌복사할 필요가 있을 때 매일 밤 완전여벌복사를 수행하는것은 불가능할수도 있다.

증분식여벌복사

증분식여벌복사는 최근에 추가되였거나 변화된 파일들만 테프에 복사한다. 이것은 마지막여벌복사가 수행된 때로부터 변화된 파일들만을 기록하여 여벌복사과정을 촉진시킨다. 대표적인 방법은 한주일에 한번 완전여벌복사를 수행하고 그다음 매일 밤 증분식여벌복사를 수행하는것이다. 봉사기를 재구성할 때에는 먼저 완전여벌복사를 진행하고 그것이 수행되면 그다음부터는 매번 증분식여벌복사를 청소한다.

증분식여벌복사의 한가지 결함은 그것이 지우기를 추적하지 못하는것이다. 이것은 가지고 있는 용량보다 더 많은 자료를 회복할수 없게 한다는것을 의미한다. 실례로 표 12-1을 보자. 파일정보가 들어 있는 12GB구동기를 가지고 있다고 하자. 월요일 첫 시간에 10GB의 파일을 이 디스크에 보관하였다. 낮에 1GB의 파일정보를 추가한다. 저녁에 완전여벌복사하여 테프에 11GB의 자료를 쓴다.

화요일 첫 시간에 12GB중 11GB의 기억용량이 쓰인것으로부터 시작한다. 낮에 1GB를 추가하고 3GB를 지웠다. 그날 마지막에 증분식여벌복사를 진행하여 1GB의 새로운 자료를 테프에 기록한다.

표 12-1　　　　　　　증분식여벌복사에서의 기억용량문제

요 일	리용된 용량	파일추가	파일지우기	테프에 보관한것
월요일	10GB	1GB	0GB	11GB
화요일	11GB	1GB	3GB	1GB
수요일	9GB	2GB	0GB	2GB
목요일	11GB	1GB	3GB	1GB

수요일 첫 시간에는 12GB중 9GB의 기억용량이 쓰이였다. 2GB의 파일을 추가하고 증분식여벌복사를 수행하여 2GB의 자료를 디스크에 기억한다. 목요일에는 1GB의 자료를 디스크에 기억하고 3GB를 지운다. 1GB의 자료를 증분식으로 테프에 여벌복사한다. 목요일 마지막시간에는 12GB중 9GB를 가지게 된다.

금요일 아침에 누군가가 12GB구동기의 모든 파일들을 지웠다는것을 발견한다. 즉시 여벌복사쏘프트웨어를 기동하여 월요일에 진행한 완전여벌복사를 회복한다. 그다음 화요일 증분테프를 적재하고 그것도 회복한다. 화요일 테프가 회복과정을 끝내기전에 봉사기로부터 《디스크공간부족》오유통보가 나타난다. 앞으로 회복하여야 할 3GB의 자료가 있는 두개의 테프가 있지만 12GB구동기에는 남은 기억공간이 없다. 이 실례에서 기억용량문제는 증분식여벌복사의 결과이다. 이러한 리유로 대부분의 체계관리자들은 증분식여벌복사대신에 차분식여벌복사를 수행한다.

차분식여벌복사

차분식여벌복사는 완전여벌복사가 마지막으로 수행된 다음부터 변화된 모든 파일들을 여벌복사한다는 의미에서 증분식여벌복사와 다르다. 차분식여벌복사는 파일들을 마지막여벌복사의 시작부터 여벌복사하지 않는다. 실례로 월요일에 완전여벌복사하고 그다음에는 매일 밤 차분식여벌복사를 진행하면 목요일 밤에 수행된 차분식여벌복사는 화요일부터 목요일사이의 모든 파일변화를 포함한다. 이것은 증분식여벌복사를 회복하는데서 본 용량문제들을 극복할수 있게 한다. 가능하지만 이 문제는 거의 제기되지 않는다.

증분식여벌복사에 비한 차분식여벌복사의 우점은 또한 봉사기가 파괴된후 두개의 테프만 회복할것을 요구한다는것이다. 이것은 처리를 촉진시키며 오유의 기회를 줄인다. 실례로 표 12-1을 보시오. 증분식여벌복사에 대하여서는 모든 자료를 회복하자면 4개의 테프들을 회복하여야 한다. 차분식여벌복사를 수행하면 2개만 하면 된다.

일러두기

테프여벌복사는 한해 또는 그이하의 테프보관기간에는 유용하다. 정보를 더 오래 기억시키려면 어떤 형태의 광학매체를 리용하거나 적당한 환경에서 테프를 보관하여야 한다.

인터네트여벌복사

여벌복사의 또 한가지 방법으로 인터네트여벌복사를 쓸수 있다. 인터네트여벌복사는 주로 원격관리되는 큰 봉사프로그람묶음에서 리용된다. Connecoted TLM과 같은 제품들

은 자동적으로 그리고 규칙적으로 암호화된 자료를 기관으로부터 복사하고 그것을 보안시설안에 있는 바깥싸이트에 보관한다. 인터네트여벌복사의 우점은 다음과 같다.

낮은 관리비용 인터네트여벌복사는 기관의 내부IT담당자의 간섭이나 감시가 없이 진행된다.

위험감소 자료는 언제나 외부싸이트에 보관되므로 현재싸이트의 재난에 의하여 자료가 영구적으로 파괴될 위험은 없다. 자료가 테프에 보관되지 않으므로 소유하고 있는 믿음직한 자료를 도적에게 잃을 위험이 보다 적어 진다.

인터네트여벌복사에는 다음과 같은 약점들도 있다.

속도 Tl를 리용한 여벌복사에서도 매우 많은 시간이 소비된다. 대역너비는 계속 증가되고 있지만 그것은 자료의 증가속도에 비해 볼 때 보잘것없는것이다. 실례로 450MB의 파일을 T1련결을 통하여 여벌복사하는데 2～3시간이 걸린다.

회복성 인터네트여벌복사로부터 자료를 회복하는데 드는 시간은 국부여벌복사에서보다 더 큰데 이것은 련결의 낮은 속도때문만이 아니다. 여벌복사봉사의 요구와 자료의 배치, 과정의 기동은 이미 느린 전송속도를 보다 더 느리게 한다.

이러한 약점에도 불구하고 일부 기관들은 인터네트여벌복사를 전반적인 자료회복해결책의 중요한 부분으로 추가하고 있으며 자료의 손실을 막는 추가적인 수단으로서 외부싸이트기억용량의 우점을 리용한다.

응용프로그람봉사제공자

응용프로그람봉사제공자(ASP)는 한가지 독특한 방법으로 봉사기고장과 자료손실문제를 해결한다. 모든 자료봉사들은 바깥에 있고 말단사용자의뢰기응용프로그람만이 기관안에서 국부적으로 실행되고 있다. 모든 자료와 봉사는 인터네트를 통하여 주관된다. ASP는 이때 자료뿐아니라 전체 응용프로그람의 리용성과 여유성을 담보할 책임을 진다.

이것은 새로 나타난 방법이지만 자기의 IT전문가나 하드웨어 및 쏘프트웨어기반을 유지할 비용이 없는 작은 기관들에 대하여서는 리상적인것으로 되고 있다. 보다 큰 기관들에서도 ASP를 리용하는것은 리득으로 되고 있다.

ASP를 리용할 때의 약점은 명백하다. 인터네트련결이 고장나면 응용프로그람이나 자료에 접근하기 위하여 의지할것이 없어 지게 된다. ASP와 관련한 계산 또는 봉사론의는 자료에 접근하지 못하며 문제가 해결될 때까지 사업이 중지된다는것을 의미할수도 있다.

또한 봉사수정은 하나의 회사에 국한된다. ASP들사이의 교환은 어려울수 있으며 자

료의 이식성은 불가능하므로 해당한 기관은 아무러한 자원이 없이 남아 있게 된다.

봉사기회복

테프여벌복사가 파일정보를 보호하는데는 좋으나 봉사기를 회복하는데 그리 효과적이지 못하다. 봉사기가 완전히 고장나고 새로운 하드웨어플래트홈에 봉사기를 재구성하여야 한다고 가정하자.

이러한 과제는 다음의 단계로 수행된다.

1. 봉사기조작체계의 설치
2. 요구되는 구동기들의 설치
3. 요구되는 봉사프로그람들의 설치
4. 요구되는 수정 및 보안프로그람들의 설치
5. 여벌복사프로그람의 설치
6. 여벌복사프로그람에 필요한 수정프로그람들의 설치
7. 완전여벌복사테프의 회복
8. 요구된다면 증분식 또는 차분식테프들의 회복

이것은 명백히 시간소비형 및 로동집약형과정이다. 이러한 과제를 하루동안에 진행한다는것은(특히 많은 량의 자료를 리용하는 경우에) 하나의 자그마한 기적이라고 말할수 있다.

한가지 방법은 봉사기회복을 위하여 특별히 설계된 프로그람묶음을 리용하는것이다. 이 프로그람묶음들은 봉사기의 원상을 따라서 몇개의 기동디스크들을 만든다. 기동디스크들은 체계가 조작체계없이 기동할수 있게 한다. 봉사기회복쏘프트웨어는 그다음 이전에 창조된 원상에 접근하여 모든 자료를 봉사기에 회복한다. 봉사기가 재기동되면 동작을 중지한다.

일부 제작자들은 봉사기회복프로그람이 여벌복사과정과 직접 통합되게 만든다. 실례로 Computer Associates의 ARCServe는 여벌복사프로그람과 봉사기회복프로그람을 둘다 가지고 있다. ARCServe를 리용하여 매일 밤 여벌복사를 수행하면 ARCServe 재난회복의 한가지 복사도 얻어 진다. 이것은 회복과정이 ARCServe여벌복사테프를 읽을수 있기때문이다. 그러므로 회복프로그람은 마지막완전여벌복사할 때의 구성으로 봉사기를 자동적으로 회복한다.

만일 봉사기회복프로그람을 다른 회사에서 구입한다면 원상파일을 따로 유지하여야 한다.

봉사기회복방법의 한가지 약점은 전체 체계를 하나의 형태로 보관한다는것이다. 이것은 여벌복사와 회복과정을 촉진하지만 또한 개별적인 파일들에 접근할수는 없다는것을 의미한다. 봉사기회복문제에 대하여서도 때때로 잃어 버린 파일을 교체하는데 규칙적인 여벌복사방법이 필요하다.

재난의 모의

지금까지는 어떻게 하면 망이 고장에 더 잘 견디도록 하며 그런 고장이 생길 때 어떻게 하면 그것을 회복할수 있겠는가에 대하여 보았다. 그러나 이것은 재난을 완전히 회복하는데 충분하지 않으며 역시 그 해결을 검사하고 문서화하여야 한다. 검사는 회복계획이 정확히 동작하도록 담보하는 유일한 방도이다. 이 과정을 문서로 만드는것은 재난이 생겼을 때 정확한 행동이 진행되도록 담보하는 유일한 방도이다.

비파괴형검사

비파괴형검사는 정상적인 사업에 영향을 주지 않고 재난방지와 회복계획을 검사할수 있게 한다. 이것은 비교적 합리적인 검사방법이다. 즉 검사가 진행되는 동안 재난이 일어 나면 안된다. 실례로 일요일 아침 9시는 봉사기의 구동기묶음의 동작중교환방법을 검사하는데 가장 좋은 시간이 아니라고 할수 있다.

재난모의의 중요성

재난회복방법을 검사하는것이 중요하다는것을 알아야 한다. 나는 언제인가 설비와 관련한 재난회복방법을 실현하려고 하는 회사와 상담한적이 있다. 그 회사는 전체 건물에 화재가 일어 나는 경우 96h동안에 원격설비에서 회복하고 정상과정에로 들어 가기를 원하였다. 원격설비가 외부싸이트테프기억으로 리용되므로 대부분의 자료가 여벌복사테프를 통하여 이 설비에로 이동되여야 하였다.

이때에는 재난을 모의할 때에만 작은 결함이라도 발견할수 있다. 기본생산봉사기에 들어 있는 DEC테프구동기는 교체봉사기의 테프구동기와 호환되지 않았다 생산봉사기의 테프구동기는 낡았으며 그 테프들을 읽을수 있는 다른 구동기를 얻을수 없었다. 이런것으로 하여 회복은 96h이상 걸렸다.

두가지 해결책이 있다.

- 생산봉사기의 테프구동기를 교체봉사기의것과 같은 모형으로 교체한다
- 테프구동기의 갱신은 두 체계에서 꼭같이 진행되여야 한다.

비파괴적검사에는 여러가지 방법이 있다. 가장 명백한것은 재난을 모의하기 위하여 또 하나의 하드웨어를 리용하는것이다. 실례로 자기의 생산봉사기와 같은 다른 봉사기를 리용하여 이 봉사기에 여벌복사를 보관할수 있다.

그러나 회복계획을 검사하기 위하여 여분의 체계를 가지기는 어렵다. 이러한 검사를 실현하기 위하여 명절이나 주말을 리용할수 있으나 실제적인 재난을 모의하기는 어렵다. 그러나 어쨌든 재난을 모의하는것은 실제적인 재난이 발생하였을 때 그것을 완전히 회복하도록 담보하는데 도움이 된다.

처리과정의 문서화

망검사를 모의하면서 오랜 시간을 보내는것보다 더 불편한 한가지 문제는 문서를 작성하는것이다. 망관리진영과 떨어 져 있으므로 매일의 회복작업을 유지하는것이 어렵다. 그러나 추가적인 재해와 문서탐색은 혼자서 모의하여야 한다. 이러한 경우에 정확한 하나의 방법에 기초하여 실제의 재해가 일어 날 때를 구체적으로 예상하여 모의하여야 한다. 손상된 봉사 또는 지워 진 정보를 다시 적재하는것이 복잡하고 시끄러운것은 사실이다. 정확한 방법을 가지고 처리과정을 문서화하여야 한다. 주의를 집중한다면 훨씬 더 빨리 이러한 문제들을 수행할수 있을것이다. 물론 여기에는 난점들을 해결하는 방법들의 탐색도 포함된다. 봉사를 재적재하는것이 어려운 경우에 처리과정을 문서화하는것은 앞으로의 봉사회복을 위하여 반드시 필요한것이다.

Windows 2000과 Windows NT에서 Octopus

Legato Octopus는 Windows 200과 Windows NT망들을 위한 실시간 자료보호와 봉사기유용성을 제공한다. 그것은 원천체계에서 선택된 파일들의 갱신내용을 포착하여 LAN이나 WAN을 통하여 사용자가 지정한 목표체계로 보낸다. 매 지정된 파일의 최근의 복사판이 원천위치에서의 자료의 손실이나 하드웨어고장에 대처하여 항상 망에 준비되여 있다.

Octopus목표가 Octopus원천이 정지되였다는것을 검출하면 Octopus목표는 그것을 대신하여 요청에 응답한다. 다시 말하여 Music라는 주식을 광고하는 Brooke라는 체계가 있으면 UNC이름(Uniform Naming Convention:단일이름짓기협약)은 \\Brooke\Music로 된다. 봉사기 Brooke가 파괴된다면 Octopus목표가 대신하여 주식 \\Brooke\Music를 광고하며 그 주식에 대한 모든 파일접근요청에 응답한다. 말단사용자가 보기에는 Brooke는 여전히 련결되여 있으며 정상동작한다. Brooke는 Network Neighborhood에 기록된다.

Octopus의 실례

Octopus는 파일들을 여벌복사하고 정보를 공유하는 몇가지 가능성을 제공한다. 실례로 그림 12-4의 망을 고찰하자. 이 그림은 두개의 원격현장사무소와 련결된 기본사무소의 망을 보여 준다. 모든 체계는 24×7점으로 동작하는데 이것은 모든 봉사기들이 모든 시간동안 련결되여 있다는것을 의미한다.

물론 이렇게 되면 밤에도 여벌복사를 위한 시간은 없는것과 같다.

사업교대시간에 여벌복사프로그람을 돌릴수 있지만 여벌복사되는 봉사기는 정확히 《책임적》이라고 볼수 없다.

여벌복사프로그람은 파일들을 될수록 빨리 복사하려고 하므로 많은 CPU시간과 디스크 I/O가 랑비된다. 이렇게 되면 사용자파일대기렬에 대한 봉사기응답시간이 매우 길어지게 된다.

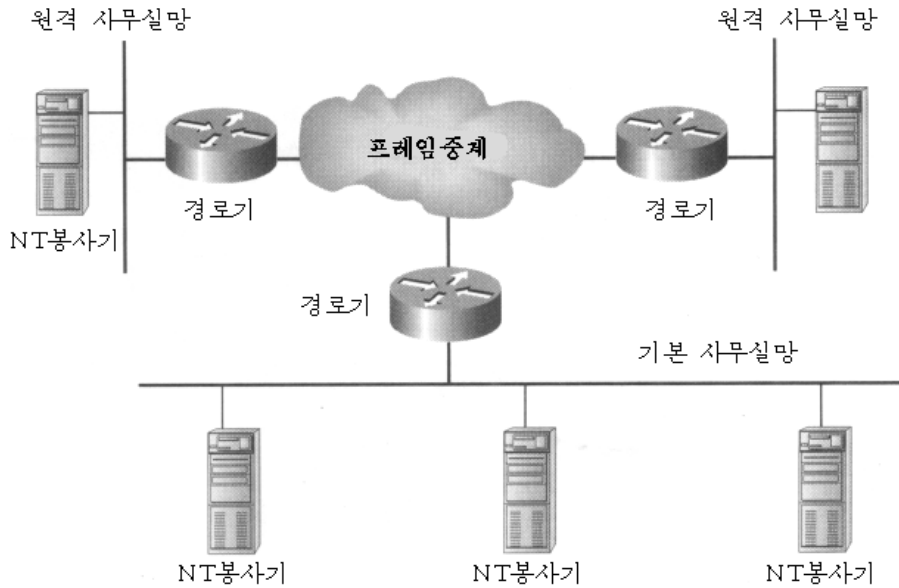



그림 12-4. 여벌복사와 100%의 리용성을 요구하는 3개의 24×7망

또 한가지의 잠재적인 리용성문제가 있다. 모든 봉사기들은 하루 24h 리용가능하여야 한다. 이 3개의 망이 프레임중계를 통하여 련결되였기때문에 프레임중계로의 매 련결은 단일고장점으로 볼수 있다. 또한 봉사기파괴와 전원차단에 약하다. 이런 재난들이 특정의 싸이트에서 발생한다면 다른 두개의 봉사기들은 봉사기자료에 더이상 접근할수 없게 된다.

한가지 해결방도는 프레임중계기밖에 새로운 마디점을 만드는것이다(그림 12-5). 이 망은 또 하나의 NT봉사기와 테프구동기를 가지고 있다. 이 체계는 Octopus목표로 구성되며 다른 모든 NT봉사기들은 Octopus원천으로 구성된다. 이 설정은 매 생산NT봉사기들로부터 원격위치에로 공유자원을 실시간으로 거울화하게 해준다.

이 실례에서 Octopus는 많은 문제들을 해결할수 있게 한다. 우선 자료가 실시간으로 거울화되며 이로 하여 디스크파괴의 효과를 최소화한다. 만일 유일한 재난해결책이 그 자료를 포함하는 봉사기밖에서 테프여벌복사체계를 돌리는것이라면 여벌복사과정이 끝난 후에 그 봉사기에서 진행된 모든 변화들은 잃어 질것이다. Octopus가 변화이후의 자료들을 즉시 거울화하므로 잃게 되는 자료의 량은 최소화된다. 테프여벌복사가 외부싸이트에서 진행되므로 여벌복사체계가 봉사기자원에 의존하는 문제도 해결된다. 이것은 테프여벌복사를 임의의 시간에 실행하여도 봉사기응답에는 영향을 주지 않는다는것을 의미한다. 이 여벌복사체계는 자기의 전용련결을 리용하므로 WAN의 대역너비는 문제로 되지 않는다.

리용가능성문제를 고찰하자. 어떤 싸이트가 정지된다고 하여도 그 싸이트에 정상적으로 보관된 자료는 아직 리용가능하다. 그것은 Octopus목표가 봉사기의 정지상태를 검출하고 그것을 대신하기때문이다. 아직 동작하는 망은 그 목표봉사기의 거울화된 복사에 접근할수 있다.

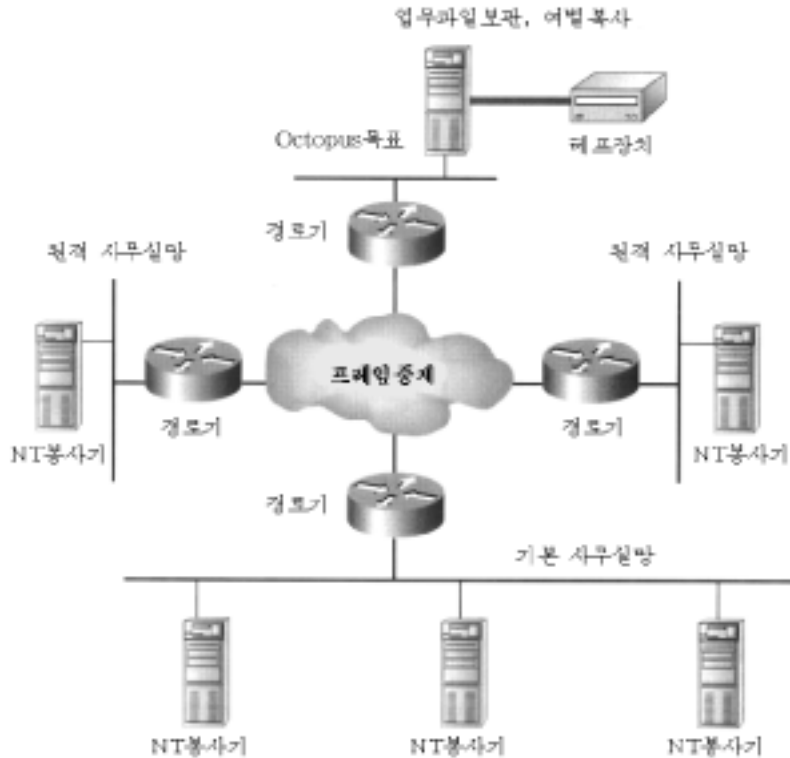



그림 12-5. Octopus는 여러 봉사기들을 원격위치에로 여벌복사하는데 쓰일수 있다

Octopus의 설치

Octopus는 Octopus목표나 Octopus원천으로 동작하는 모든 체계에 설치되여야 한다.

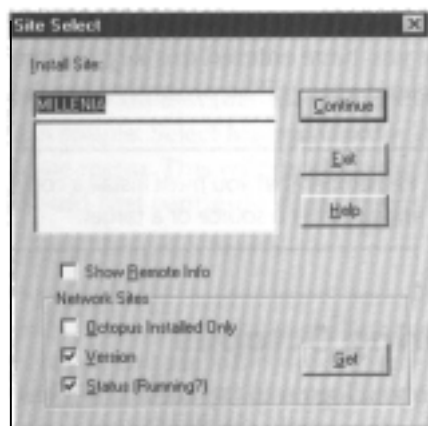



그림 12-6. Octopus Site Select대화칸

설치과정을 시작하기 위하여 CD를 NT봉사기에 넣고 setup을 실행한다. 이때 그림 12-6과 같은 Site Select대화칸이 나오며 이때 Octopus를 설치하려는 체계의 Microsoft 기계이름을 입력하여야 한다. 봉사기이름(그림과 같이)을 입력할수도 있고 Get단추를 눌러 망에서 NT봉사기들을 검색할수도 있다. 대화칸의 Network Site부분은 Get에 의하여 얻은 정보를 설정하게 하여야 한다. 정확한 봉사기이름을 입력한 다음 Continue를 찰칵한다.

일러두기

망에서 NT봉사기를 검색하기 위하여 Get를 리용하면 처리속도가 떠진다. 가능하다면 봉사기이름을 직접 입력하는것이 좋다.

다음에는 그림 12-7과 같이 프로그람과 자료파일들의 경로를 선택하여야 한다. 이 기억위치들은 Octopus프로그람에 의하여서만 리용된다. 어느 부분을 거울화하려는가를 식별하면 목표체계에 목적지를 선택할수 있다. 파일경로를 입력하였다면 Continue단추를 찰칵한다.

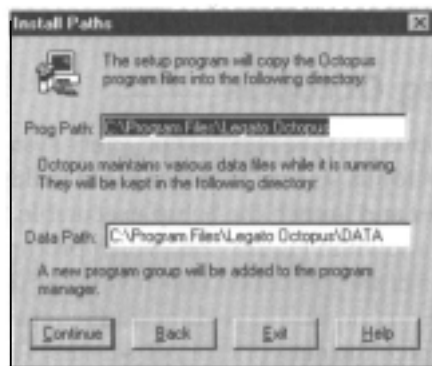



그림 12-7. 설치경로대화칸

마지막대화칸은 사용권열쇠를 요구한다. Qualix Group의 Web싸이트(www.octopustech.com)를 방문하거나 Qualix Group을 직접 접촉하여 사용권열쇠를 얻기 위한 제품계렬번호를 받아야 한다.

이 열쇠를 입력하면 프로그람파일은 하드구동기에 복사되며 NT봉사기를 재기동하라는 지령이 나온다.

주 의

원천이나 목표로 동작하는 매 봉사기에 Octopus의 복사를 설치하여야 한다는것을 잊지 말아야 한다.

Octopus의 구성

2000이나 NT봉사기에 가입하고 Octopus그림기호를 찰칵하면 그림 12-8과 같은 Octopus조종탁이 나타난다. 모든 공유응답은 Octopus원천에서 구성되며 따라서 만일 현재 원천의 조종탁이 아니라면 조종탁차림표에서 Functions→Attach를 선택하여 원천체계에 련결할수 있다. 이때 제품설치에서와 같은 Site Select 대화칸이 나온다. 자기가 련결하려는 Octopus원천 NT봉사기의 이름을 입력할수도 있고 Get단추를 찰칵하면 설치된 Octopus를 가진 NT봉사기를 망에서 검색할수도 있다. 자기가 목적하는 원천을 찾으면 조종탁은 그 체계에 대하여 능동으로 된다.

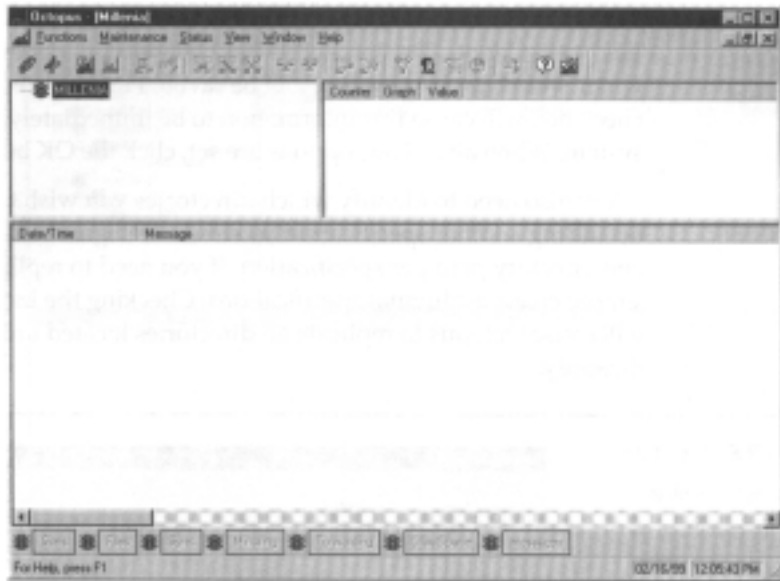



그림 12-8. Octopus조종탁화면

다음에는 어느 정보를 복사하여 어느 원천에 보내겠는가를 확인하는 일람표를 추가하여야 한다. Octopus조종탁차림표의 Maintenance → Add Specification → Share를 선택한다.

이때 그림 12-9와 같은 Mirror Shares 화면이 나온다. 먼저 자기의 체계를 모든 공유정보를 복사하도록 구성하여야 한다.

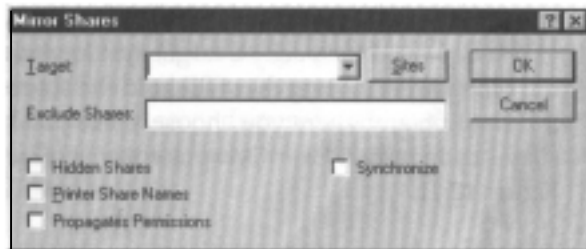



그림 12-9. Mirror Shares 화면에서 공유복사

경 고

Octopus는 일의적인 공유이름들만 거울화한다. 이것은 같은 목표를 공유한 2개의 Octopus원천이 같은 이름의 공유를 가지지 말아야 한다는것을 의미한다. 만일 공유되면 충돌을 피하기 위하여 공유들중 하나가 무효로 된다.

Exclude Shares 마당은 복사하지 않으려는 어떤 공유를 기록한다. 관리공유를 제외한 모든 공유를 보관하려면 이 항목을 공백으로 남긴다. Target Site 마당은 이 공유정보가 기억된 Octopus목표를 확인하게 한다. 마지막으로 Synchronize검사칸을 선택하면 이 정보는 즉시 목표체계에로 복사된다. 모든 항목들이 설정되면 OK단추를 누른다.

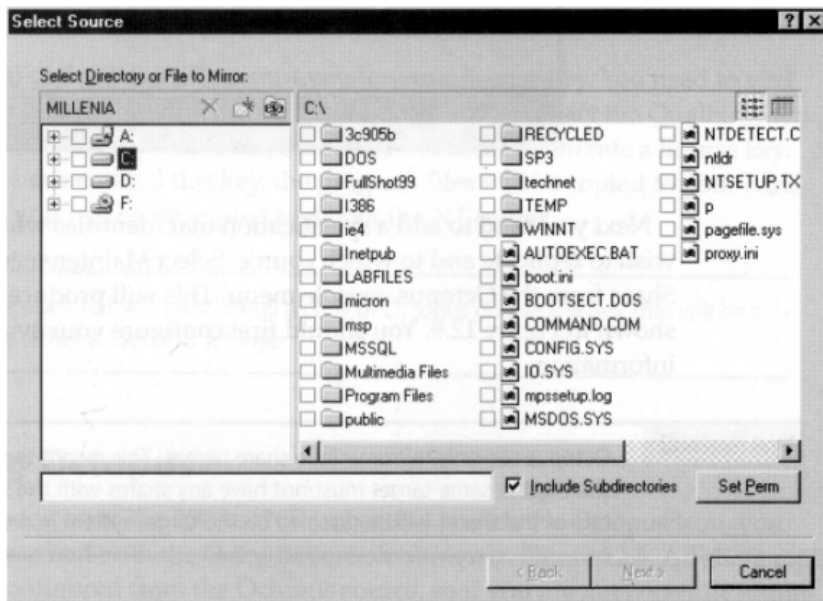



그림 12-10. Select Soure화면을 리용한 파일복사

또한 어느 등록부를 복사하겠는가를 확인하여야 한다. 이것은 그림 12-10과 같은 또 하나의 명세를 추가하여 수행한다. 매 명세에서 오직 하나의 등록부만을 기록할수 있다. 여러개의 등록부를 복사하려면 추가적인 명세를 만들어야 한다. Include Subdirectories칸을 검사하면 Octopus는 기록된 원천등록부안에 위치한 모든 등록부들을 복사한다.

또한 목표체계와 목표등록부를 지정하여야 한다. 이것은 공유하는 같은 목표체계로 되지만 등록부정보를 자기가 선택하는 곳에 놓을수 있다. 마지막에 OK를 찰칵하여 요구되는 공유들을 추가한다. Octopus조종탁화면은 그림 12-11와 같다.

Octopus조종탁의 왼쪽창문은 Octopus원천이 목표체계 LAB31을 복사하게 설정되였다는것을 보여 준다. 색(푸른)갈은 이 체계들이 여전히 서로 통신할수 있다는것을 보여 준다. 목표체계하에서 자기가 구성한 모든 명세들을 볼수 있다. 이 실례에서는 labfiles등록부를 복사한다.

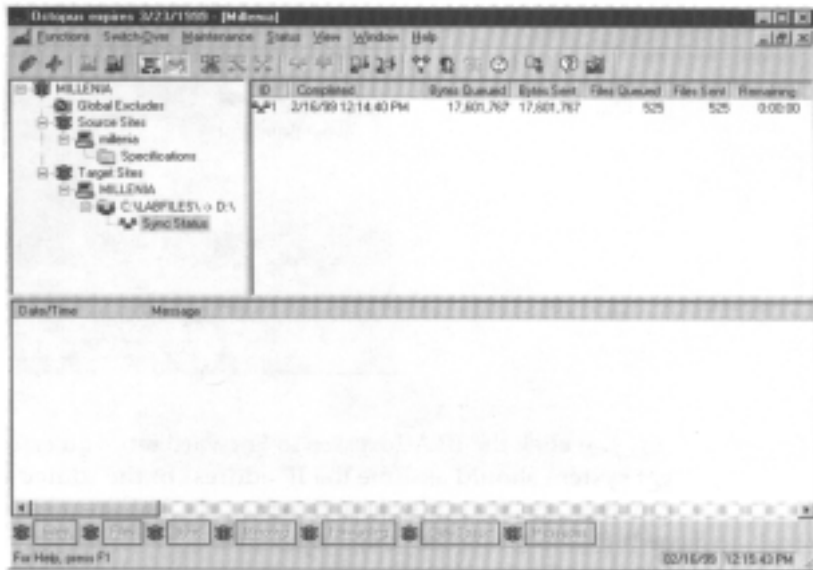



그림 12-11. 등록부명세를 가진 Octopus조종탁

오른쪽창문은 우의 창문에서 강조한 명세의 현재 복사상태를 보여 준다.그림 12-11로부터 Octopus가 labfiles등록부에서 525개의 파일들을 찾아서 복사하였다는것을 알 수 있다.

이제는 파일정보가 복사된 상태에서 고장이 생기는 경우 어떻게 응답하겠는가를 Octopus체계에 알려 주어야 한다. 그러자면 Octopus조종탁화면의 Switch-Over → Source를 선택한다. 그러면 그림 12-12와 같은 Source Option대화칸이 나온다.

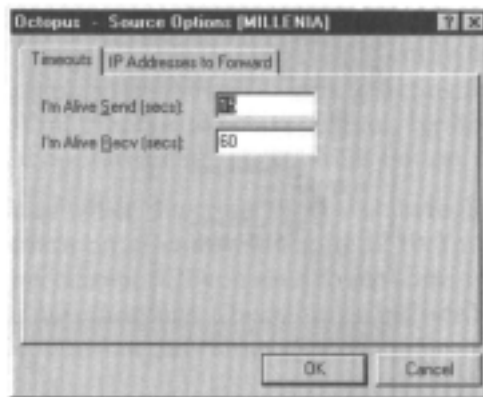



그림 12-12. Source Options창문

Timeout칸은 원천과 목표체계사이의 통신파라메터들을 설정한다. 그림 12-12는 원천이 15s에 한번씩 신호를 전송한다는것을 보여 준다. 목표는 신호를 60s동안 받지 못하면 원천이 정지되였다고 가정한다. 이것은 하나 또는 두개의 파케트손실이 전체 과정에 영

향을 주지 않도록 한다.

만일 IP Addresses to Forward칸을 찰칵하면 고장이 생기는 경우 목표체계가 원천체계의 IP주소를 가정하여야 하는가를 지정할수 있다. 지어 여러개의 망기판들을 지적할수도 있다. 이것은 원천체계를 지적하는데 DNS나 WINS를 리용하는 체계들이 고장이 발생한후에 목표체계에로 지향되도록 담보한다.

주 의

만일 2개의 체계가 같은 국부망에 위치하면 목표는 원천의 IP주소만을 가정할수 있다.

마지막칸은 Cluster To인데 이것은 목표체계를 지적하게 한다. 만일 명세를 만들었다면(앞에서 한것과 같이) 이 값은 채워 져 있으며 변화시킬 필요가 없다. Souce Option을 다 구성하였다면 OK를 찰칵하여 그 변화들을 보관한다.

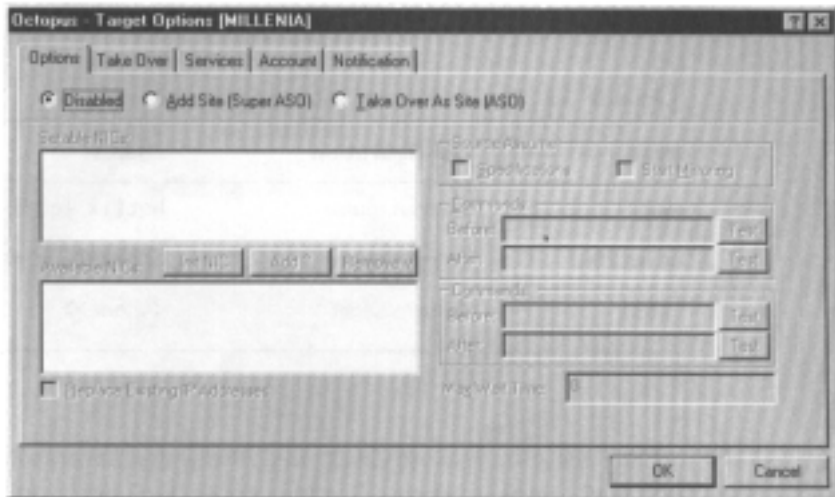



그림 12-13. Target Options창문

마지막으로 목표체계를 위한 선택안들을 구성하여야 한다. 그러자면 Octopus조종탁화면의 Switch-Over → Target Options를 선택한다. 이때 그림 12-13과 같은 Target Options대화칸이 나온다.

Option 칸은 목표가 다른 체계들에 어떻게 응답하는가를 구성할수 있게 한다. 여기서 실행파일 또는 묶음파일을 정의할수 있다. 또한 목표가 자기의 IP주소를 원천의 IP주소로 교체하겠는가 또는 두개 주소를 동시에 리용하겠는가를 결정할수 있다. Take Over칸을 누르면 이 목표가 넘겨 받은 현재의 원천들을 볼수 있다.

Services칸은 고장극복이 진행되였을 때 어느 봉사기가 목표체계우에서 돌아 가는가를 지적할수 있게 한다. 기정에 의하여 목표가 원천을 대신할 때 목표체계우의 모든 봉사들은 재시동된다. 이것은 Octopus목표가 요구되는 기계이름과 IP주소를 가정하게 한

다. 그러나 어떤 봉사들은 재시동되지 않으며 지어 어떤 봉사들은 고장극복이 필요할 때에만 동작하도록 지정할수 있다.

Account 칸은 인증정보를 넣기 위한것이다. 이것은 원천이 독립봉사기이고 목표가 새로운 System ID(SID)를 제공하여야 할 때에만 필요하다. 원천이 PDC나 BDC이라면 이 정보는 필요하지 않다.

Notification칸은 목표가 원천을 대신할것을 누구에게 통지할것인가를 지정하게 한다. 어떤 전자우편주소나 NT가입자이름 또는 전체 령역에로 통보문이 전송될수 있다.

Target Option을 완성하면 OK를 눌러서 변화률을 보관한다. 원천과 목표체계들은 지금 재난이 발생하는 경우 봉사기준위의 고장견딤성을 제공하도록 구성되였다.

Octopus의 검사

고장극복이 말단사용자들에게 어떻게 보이는가를 보여 주기 위하여 3개의 Octopus검사체계를 구성하였다. 그중 2개(www와 holnt 200)는 Octopus원천이고 세번째(lab31)는 Octopus목표로 설정되였다. 표 12-2는 매 체계에서 쓰이는 공유이름들을 보여 준다.

표 12-2 Octopus검사체계에서 리용되는 공유이름들

호스트	구 성	공 유
www	Octopus원천	hotfix, labfiles
holnt200	Octopus원천	accounting, marketing, last_share
lab31	Octopus목표	<<none>>

원천이 구성되면 체계는 복사가 끝날 때까지 동작하지 않는다. 복사과정은 10min이하 걸린다. 이 처리가 끝나면 lab31은 두 Octopus원천에 위치한 매 공유의 복사를 가지게 된다. 이 공유의 Network Neighborhood는 그림 12-14와 같다.

그림 12-14. 모든 공유들의 복사를 가지는 lab31

그다음 봉사기 www와 holnt200우에서 전원접속구를 뽑으면 이 두 원천체계들이 정지되였다는것을 목표체계가 리해하는데 1min간 걸린다(이것은 구성된 교대시간이다). 1min후에 두개의 원천체계들이 더이상 반응하지 않는다는것을 알리는 통보들이 령역관리자에게 전달된다. Octopus조종탁화면으로부터 Switch-Over → Target Options → Take Over를 검사하면 lab31이 www와 holnt200을 대신한다는것을 볼수 있다.

그림 12-15에서와 같이 이 과정은 이미 완성되였다. Added Names마당은 목표체계가 어느 원천체계를 대신하는가를 보여 준다.

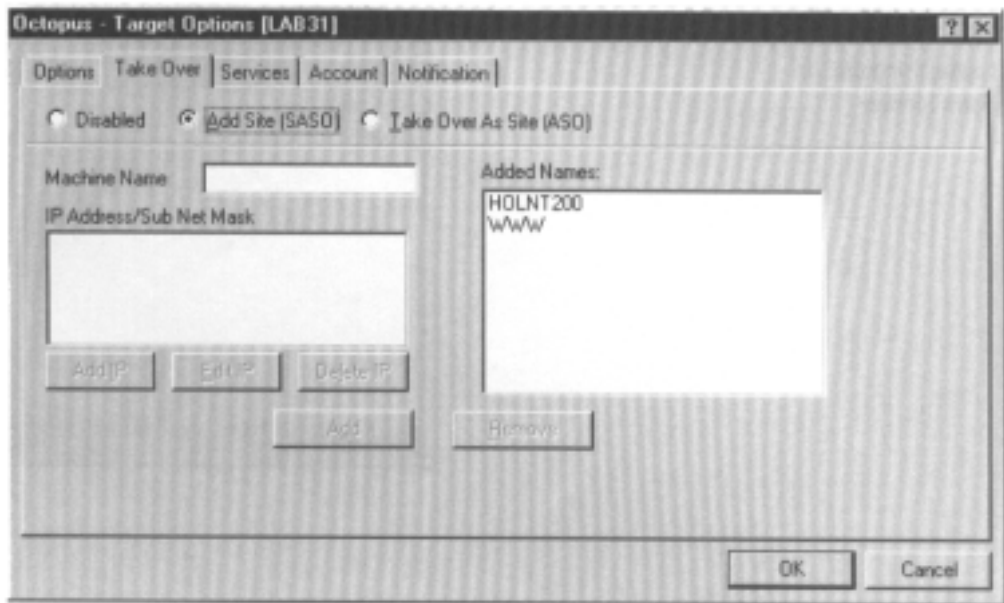



그림 12-15. Target Option Take Over표쪽

목표가 원천체계들을 대신하였다는것을 확인하기 위하여 Windows 95 검사체계로부터 Network Neighborhood를 기동하였다. 그림 12-16에서 보여 준바와 같이 의뢰기 hellsfarr는 모든 봉사기들이 아직 련결되여 있고 동작하고 있는것으로 생각한다. Neighborhood검색을 위한 응답시간은 그 봉사기들이 실제로 련결되여 있을 때보다 길지 않다.

마침내 www와 holnt 200은 정확한 공유이름들이 정확한 체계들과 결합되였다는것을 담보한다는것이 확인되였다.

그림 12-16. lab31로 www와 holnt 200을 대신

그림 12-17에서 보여 준것처럼 lab31은 체계 www와 정확한 공유이름으로 결합되였다. 매 공유를 열면 기대되는 파일목록이 얻어 진다.

그림 12-17. www의 정확한 공유를 보여 주는 lab31

요 약

이 장에서는 망을 보호하는데 어떤 재난방지와 재난회복방법들이 준비되여 있는가를 고찰하였다. 먼저 망에 대한 재난과 봉사기에 대한 재난을 고찰하였다. 또한 재난회복에서 검사 및 문서화의 중요성에 대하여 설명하였다. 마지막으로 NT봉사기환경에서 여벌봉사기를 리용하여 고장견딤성을 제공한다는것을 고찰하였다.

다음장에서는 Novell NetWare조작체계에서 어떤 위험성이 존재하며 그것을 막기 위하여서는 어떻게 하여야 하는가에 대하여 설명한다.

제1 3장. NetWare

1983년에 개발된 NetWare는 파일과 인쇄기봉사를 제공하는 대부분 망들에서 주역을 담당하고 있다. Novell회사는 4.11판본에서 인트라네트라고 부르는 내부인터네트를 구성할수 있도록 일부 IP응용을 지원하였다. 인트라네트는 자원접근이 내부인원으로 제한된다는 점을 제외하고는 인터네트(HTTP, FTP 등)와의 련결을 실현할수 있는 많은 기능들을 제공한다.

NetWare는 5.0판본(현재는 5.1판본이 개발)에서 IP규약의 고유한 기능들을 모두 지원하였다. NetWare가 NetWare IP를 리용하여 IP에 기초한 의뢰기통신을 지원한다고 할 때 NetWareIP는 단순히 IPx자료흐름을 보장하는 IP통로에 지나지 않는다. 즉 NetWare 5.0판본은 외견상 IPx를 완전히 제거하였다고 볼수 있다.

NetWare봉사기의 기정보안기능은 아주 견고하다. 파일체계는 허가속성을 구체적으로 세분화하여 지원하고 있으며 일반 사용자에게는 체계자원에 대한 접근을 거의 허용하지 않는다. 그러나 철저한 보안을 실현하기 위하여서는 여러가지 문제들을 고려하여야 한다.

NetWare핵심부OS

NetWare의 핵심부는 32bit, 다중과제, 다중스레드용으로 설계되였다. 대칭형다중처리기지원이 핵심부OS에 포함되여 있으며 핵심부는 모듈방식으로 설계되였다. 모듈방식을 리용함으로써 응용프로그람들과 지원구동기들이 원활하게 적재, 제거될수 있다.

주　의

이것은 IP주소변환과 같은 대부분의 체계변화가 재기동없이 사용할수 있다는것을 의미한다. NetWare에서 IP주소변환은 지령대기상태에서 2개의 지령으로 이루어 지며 즉시사용이 가능하다. 이러한 환경구조기능은 수시로 체계변경이 요구되지만 중단 없이 주야봉사를 보장하여야 하는 봉사기인 경우 아주 유용하다.

NetWare 5.0판본은 Java도 지원한다. Novell의 Java가상기계(JVM)는 봉사기에서 Java기반응용프로그람의 개발과 실행을 가능하게 한다.

4.x판본까지의 NetWare에서는 모든 프로그람들이 봉사기의 주기억에 적재되여 실행되도록 설계하였다. 다시 말하여 교체공간 또는 가상기억을 지원하지 않았다. 그러므로 조작체계가 사용할수 있는 주기억은 봉사기에 물리적으로 설치한 주기억으로 제한되게 된다.

주　의

NetWare5.0에서는 가상기억을 지원한다.

주기억은 NetWare봉사기에서만 사용하지 않는다. 응용프로그람을 지원하는 핵심OS와 구동기의 적재, 의뢰기들이 자주 접근하는 파일들의 완충을 위하여서도 사용된다. 사용자들이 공통적으로 리용하는 파일들은 디스크보다 속도가 더 빠른 주기억에 배치하고 접근봉사를 처리한다. 조작체계가 추가로 주기억공간을 요구할 때에는 파일완충용공간으로부터 일부를 떼내여 리용한다.

Novell은 또한 비정상완료(ABEND)라는 치명적인 체계오유를 회복하는 기능도 개선하였다. NetWare의 이전 판본들에서는 이런 오유발생시 봉사기가 모든 처리를 정지시킨다. 유일한 회복방법은 직결오유축적기를 통하여 봉사기를 재기동하는가 아니면 완전히 전원을 끄고 다시 재기동하는것이다.

NetWare에는 또한 ABEND오유가 발생하면 규정된 주기시간후에 봉사기를 재기동하는 기능도 있다. 어떤 종류의 ABEND오유에 의하여 봉사기를 재기동시키겠는가를 선택할수 있다. 실례로 봉사기가 응용프로그람에서 발생한 ABEND오유를 단순히 회복하도록 설정할수 있다. 그러나 장치와 련관된 오유라면 봉사기는 재기동한다.

NetWare는 휴지통수집기능을 설정할수 있다. 이 기능은 정지되지 않는 한 제거된 프로쎄스로부터 기억을 회수하여 다른 프로쎄스가 리용할수 있는 자유기억공간으로 복귀시킨다.

NetWare의 이전 판본들에서는 잘못 작성된 응용프로그람이 주기억에서 제거될 때 응용프로그람이 자기가 리용하던 기억공간을 모두 자유기억공간으로 복귀시키도록 설계하지 못하였다. 이것은 조작체계우에서 동작하는 응용프로그람들에서 공통적인 문제이다. 휴지통수집처리는 더이상 리용하지 않는 주기억범위를 조사하고 발견하면 지적자를 지우고 다른 응용프로그람이 리용할수 있도록 자유기억공간으로 복귀시킨다.

새로운 특징은 또한 응용프로그람이 오래동안 처리기를 독점하지 않도록 설계한것이다. NetWare에는 응용프로그람이 CPU의 공유와 공평한 리용이 거절될 때 오유통보문을 발생하는 조종포기경보설정이 있다. 또한 CPU독점시간초과설정에 의하여 봉사기의 처리기시간을 전부 독점하는 그러한 프로쎄스를 자동적으로 소멸하도록 한다.

C2증서

NetWare는 국가콤퓨터보안쎈터(NCSC)가 공인하는 C2증서를 받아 들인 분산형망조작체계이다. NT도 C2증서를 받아 들였지만 이 책이 출판되면 NT는 신뢰할수 있는 망으로서는 공인되지 못하고 조작체계측면에서만 인정된다. 다시 말하여 망련결 또는 매체련결이 없는 단독워크스테이션으로서만 인정된다. NetWare는 전자자료(Electronic Data)의 E2등급으로 평가되고 있다. E2은 C2의 유럽사본인데 매개 증서들은 거의 류사하다.

C2명세

NCSC가 신뢰하는 C2등급의 망으로 공인되기 위하여서는 다음의 명세들에 부합되여야 한다.

- 체계는 매개 체계사용자들을 유일하게 식별할수 있어야 한다.
- 체계는 사용자가입과 대상의 변경을 선택적으로 추적할수 있어야 한다.

- 체계는 조사를 위하여 추적된 정보를 유지할수 있어야 하며 그러한 정보는 매 입구점의 원천(어느 원격체계, 말단, 봉사기조종탁)들을 구별하여야 한다.
- 체계관리자는 조사를 위한 정보에 대하여서는 사용자들의 접근을 제한할수 있어야 한다.
- 체계에는 개별적으로 또는 그룹단위로 접근조종을 설정하는 방법이 있어야 한다.
- 체계관리자는 접근조종권한을 제한할수 있어야 한다.
- 체계관리자는 체계가 정상가동한다는것을 검증할수 있어야 한다.
- 체계는 모든 보안특징을 서술한 지도서를 가지고 있어야 한다.
- 보안특징은 NCSC에 의하여 검사되고 결함이 없다는것이 증명되여야 한다.

C2등급에 복종시키는데서 결함이 없다는 마지막규정은 문제로 된다. C2증서는 해커가능성을 완전히 제거한다는데 대하여서는 담보하지 않는다. 그러나 보안을 고려하여 설계하였으므로 이러한 보안예방을 제3자의 정부기관에서도 리용할수 있다는데 대하여서는 언급하고 있다.

NetWare등록부봉사

NetWare는 접근조종을 위하여 NetWare등록부봉사(NDS)를 사용한다. NetWare등록부봉사는 망접근권한을 할당하고 관리하는데 계층수법을 리용한다. 그러므로 전체 망환경을 하나의 조종탁에 의하여 관리하게 된다. NetWare등록부봉사는 또한 망자원에 대한 사용자련결을 구체적인 세부준위까지 조종할수 있는 기능을 제공한다. 기관의 NDS구조를 보통 NDS나무라고 한다.

NDS의 구조는 하드구동기의 등록부구조와 류사하다. 기관단위 또는 용기로 볼수 있는 부분등록부는 뿌리아래에 정의된다. 접근권한은 사용자들이 자기가 필요한 망자원에만 접근할수 있도록 부분등록부단위로 설정될수 있다. 사용자접근을 더 구체적으로 관리하기 위하여서는 더 많은 부분등록부를 정의하여야 한다.

주 의

부분등록부에 대하여 총관리자와 같은 특권을 가진 부분관리자를 임명할수 있다. NDS는 큰 기관에서 지정된 그룹마다 자기자원을 관리하는 관리자를 설정할수도 있고 또한 완전한 관리권환을 전체 망관리를 책임진 여러 관리자들에게 부여할수 있도록 체계화가 잘되여 있다. 권한은 웃준위기준에 기초하여 배당된다. 즉 현재 권한이 부여된 등록부내의 모든 부분등록부들에 대하여 특별히 설정을 하지 않는 한 같은 권한이 부여된다.

망접근은 또한 집중화되여 있다. 사용자가 망에 가입하면 특정봉사기 또는 나무의 어떤 부분이 아니라 전체 NDS나무에 대하여 인증된다. 이것은 할당된 모든 망자원에 대한 접근이 가능하다는것을 의미한다. 심지어 NDS나무에 원격인쇄기와 같은 원격자원이 존재한다고 하여도 사용자에게 할당된 자원이라면 접근이 가능하다.

NDS설계

NDS나무가 어떻게 구성되여야 하는가 하는 실례를 그림 13-1에서 보기로 하자. Cam기관은 위치상 5개의 지역 즉 알브큐에르큐, 보이스, 로스안젤스, 솔트레이크시, 탐파로 나누어 진다. 매 등록부에 대한 접근을 할당 받은 사용자는 해당 지역의 모든 자원에 접근할수 있다. 매 지역이 자기의 IS담당자를 가진다면 해당한 등록부에 IS담당자의 구좌를 창조한다. 등록부안에 이러한 관리자들을 정의함으로써 해당 지역의 모든 자원을 관리할수 있다. 그리고 Cam등록부에 직접 사용자구좌를 여러개 창조하여 전체 나무를 관리하도록 할수 있다.

매 지역에서 자원을 부서단위로 취급하기 위하여 더 많은 부분등록부들을 정의할수도 있다. 이렇게 하여 지역안에서 망자원을 세분화하여 관리할수 있다. 실례로 그림 13-1에서 HQ등록부를 보자. HQ등록부에는 사용자그룹들과 이들이 접근하는 인쇄기, 파일, 응용프로그람자원들이 정의되여 있다. 이와 같이 NDS나무에서는 접근요구에 기초하여 망객체를 관리함으로써 보안관리를 단순하게 한다.

NDS에서는 사용자가 여러 등록부들에 접근할수도 있다. 실례로 한 사람이 Cam회사의 부기원이고 모든 재정자료에 대한 접근을 요구한다고 하자. 이 사람에게 NDS나무 전체에 대한 접근을 할당한다면 자기가 소속되지 않은 지역들에서는 모든 등록부들을 탐색하여야 재정자료를 찾을수 있다.

그림 13-1. NDS나무의 실례

NDS에서는 하나의 등록부에서만 그것을 위한 사용자대상을 실지로 창조하고 다른 지역의 필요한 등록부들에서는 실제의 사용자대상을 지적하는 가명을 리용한다. 그림 13-1에서 부기원대상은 다른 등록부에서 창조된 실제대상을 지정하는 가명이다. 이러한 방법으로 필요한 자원에만 접근하도록 할수 있다.

구 좌 관 리

NetWare 5.0에서부터는 사용자구좌를 Java도구프로그람인 Consoleone에서 관리한다. NetWare 4.x에서는 NetWare관리자(nwadmin)를, NetWare 3.x에서는 syscon을 리용하였다. Console One이 봉사기에서 실행되므로 부분적으로 구좌관리를 담당하는 워크스테이션들이 필요없게 된다.

그러나 구좌관리는 좀 복잡해 진다. 특정사용자에 대한 모든 보안설정을 보기 위하여서는 단순히 사용자대상에 대한 오른쪽찰칵하여 상세하게 선택하면 된다. 그러면 그림 13-2와 같은 사용자정보화면이 펼쳐 진다.

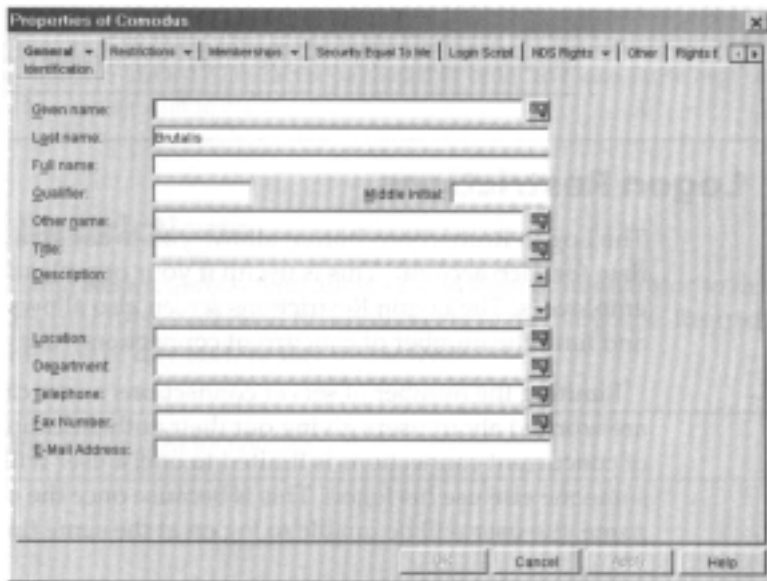



그림 13-2. Console One에서 Comodus사용자의 관리

이 조종탁에서 통과암호제한, 파일접근권한, 지어 사용자가입정보서술과 같은 사용자구좌의 모든 항목들을 관리할수 있다. 다음의 단락들에서는 이 조종탁에서 할수 있는 일부 보안관리들에 대하여 설명한다.

식별

식별단추에서는 사용자정보를 등록한다. 사용자정보에는 다음의 요소들이 포함된다.

- 전체 이름

- 위치
- 부서
- 전화번호
- 사용자의 직속관리자와 같은 서술정보

상세한 사용자정보등록이 외견상 보안특성과는 관련이 없는것 같지만 보안문제를 추적할 때에는 아주 중요하게 리용된다.

가령 체계를 조사하여 사용자구좌 jsmith로부터 오는 어떤 의심스러운 동작을 추적한다고 하자. 조사과정에 jsmith가 부기자료기지에 대한 접근획득을 시도하였다는것이 밝혀진다. Console One을 리용하여 jsmith사용자정보를 찾고 그가 구내전화번호 1379에 있는 Toby Miller로 기록한다는것을 알아 낸다. 이 정보에 기초하여 신속히 Toby에게 전화를 걸어 jsmith의 부기자료기지에 대한 접근시도를 현행으로 잡도록 할수 있다.

일러두기

체계조사를 할 때 상세한 사용자정보는 아주 중요하다. 그것은 사용자들의 가입동작과 경과기록정보를 서로 련관시킬수 있기때문이다. 규모가 큰 환경에서는 체계관리자가 모든 가입이름들을 기억해야 하므로 불리하다.

가입제한

가입제한단추에서는 매 구좌에 대하여 미리 결정된 만기날자를 배당한다. 이 기능은 기관에서 림시직원을 채용하는 경우 효과적이다. 가입제한화면에서는 또한 매 사용자가 가지고 있는 구좌를 무시하거나 동시련결수를 제한하게 할수도 있다.

사용자의 봉사기련결수를 제한하는 기능은 사용자들이 자기의 인증증서을 배포하는것을 금지시키는데서 효과적이다. 가령 동시련결수를 1로 제한했다면 사용자가 자기의 가입을 다른 사람이 리용하게 하는것을 금지시킬수 있다. 그것은 같은 이름으로 동시에 두번이상 가입하는것이 가입제한설정으로부터 금지되였기때문이다.

동시련결제한은 또한 훔친 구좌를 알아 내는 아주 좋은 방법이다. 사용자가 가입을 시도하여 자기가 또 다른 체계로부터 가입이 되여 있다는 통보문을 받았다면 관리자에게 통보하여 잠재하는 공격자를 추적할수 있다.

통과암호제한

통과암호제한단추에서는 사용자의 통과암호를 구체적으로 정의한다. 설정할수 있는 파라메터들은 다음과 같다.

- 사용자가 자기의 통과암호를 변경할수 있는가를 허용
- 구좌에 통과암호리용이 요구되는가를 정의
- 통과암호의 최소문자수를 정의
- 구좌가 여러개의 통과암호를 리용할수 있는가를 허용

• 통과암호가 얼마나 자주 변경되는가를 정의
• 구좌를 잠그기전까지의 불법가입시도의 회수를 정의
• 구좌의 현재 통과암호를 변경

알려두기

NDS에서 통과암호제한은 아주 유연하다. 즉 사용자부류별로 파라메터를 정의할수 있다. 실례로 일반 사용자들에 대해서는 6개문자이상의 통과암호, 망관리자에 대해서는 12개문자이상의 통과암호를 사용하게 할수 있다.

가입시간제한

가입시간제한화면에서는 사용자가 언제 NDS나무에 인증될수 있는가를 정의한다. 제한은 매일 어느 시간 또는 매주 어느 날로 설정할수 있다.

주 의

NDS는 명절들에 대하여서는 정의하지 않는다.

실례로 그림 13-3에서 체계관리자는 Comodus사용자가 망자원에 언제 접근할수 있는가를 규정하고 있다. Comodus사용자는 월요일부터 금요일까지는 오전 7시부터 오후 6시까지, 토요일에는 오전 8시부터 낮 12시까지에만 가입이 허용된다. 그밖의 시간에는 망에 가입할수 없다. 시간주기가 만기되는 시간에 사용자가 여전히 가입하고 있다면 5min간 경고를 보낸 다음 련결을 차단한다.

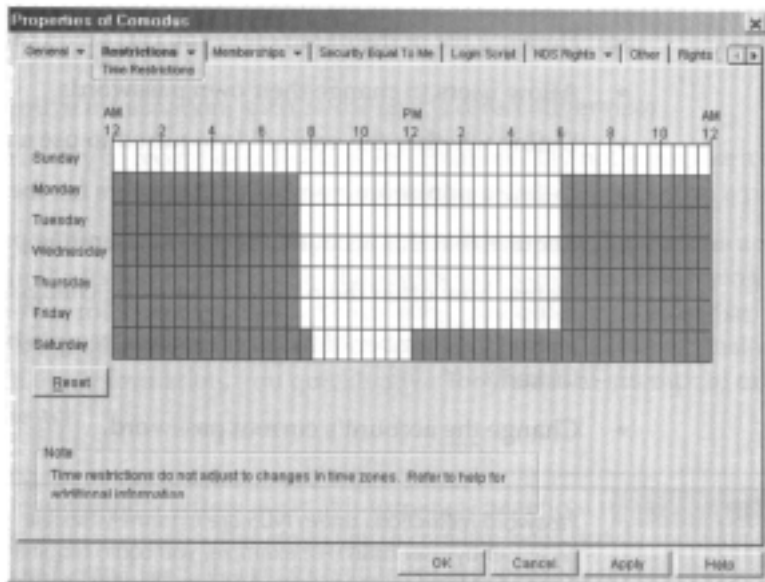



그림 13-3. 가입시간제한화면

시간제한은 여벌복사처리를 기동하기 전에 사용자들을 체계에서 탈퇴시키는 좋은 방법이다. 체계에 가입한 사용자는 열린 파일들을 가지게 된다. 여벌복사처리프로그람들은 정확한 여벌복사처리를 위하여 파일정보에 대한 배타적접근이 필요하므로 열린 파일들에 대하여서는 여벌복사처리를 할수 없다. 시간제한을 리용하여 여벌복사처리프로그람을 기동하기전에 사용자들은 망에서 탈퇴시킬수 있다.

망주소제한

망주소제한단추에서는 사용자들이 NDS나무에서 인증될 때 어떤 체계를 리용하는가를 정의한다. 그림 13-4와 같이 망관리자는 사용자가 지정한 망규약을 리용하도록 제한한다. 즉 사용자는 지정한 규약으로만 망자원에 접근할수 있다.

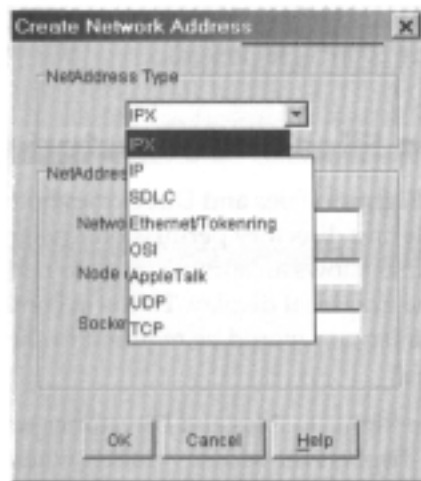



그림 13-4. 망주소제한화면

실례로 전용체계에서 동작하는 응용프로그람을 리용하는 사용자가 봉사기의 접근을 위하여 통과암호가 없는 하나의 구좌를 가진다고 가정하자. 이러한 경우 체계가 재기동한다면 통과암호를 요구함이 없이 즉시에 망자원접근이 가능하게 된다.

통과암호가 없는 구좌는 명백히 보안상 위험하다. 그러나 이 구좌가 상대적으로 안전하다는것을 보증하는 예방책을 취할수 있다. 전용체계의 가입만을 허용하는 구좌에 대하여 망주소제한을 정의함으로써 구좌는 안전하게 된다. 즉 워크스테이션에는 물리적인 안전이 제공된다. 이러한 기능은 다른 위치에서 이 구좌를 리용하여 망에 가입하는것을 차단할수 있게 한다.

침입자차단

침입자차단단추에서는 실패한 가입시도들에 대한 통계정보를 보여 준다. 체계관리자는 부정확한 통과암호를 리용하여 가입을 시도한 구좌들과 콤퓨터주소들을 조사할수 있다. 이러한 기능은 침입자를 추적하는 아주 쓸모 있는 정보이다.

주　　의

실패한 가입시도들은 경과기록정보에 등록된다.

구좌가 차단되지 않은 경우에도 실패한 시도의 회수와 오유계수기가 0으로 설정되기 전의 마지막시간값(가입에 소요된 시간)들을 조사할수 있다.

파일과 등록부에 대한 권한

파일과 등록부에 대한 권한단추를 리용하여 NDS관리자는 사용자들에게 할당한 모든 파일과 등록부들에 대한 허가정보를 조사한다. 관리자는 이 기능을 리용하여 하나의 화면상에서 모든 사용자들의 접근권한을 조사할수 있다. 그러나 이 기능은 모든 등록부, 모든 봉사기를 조사하는 Windows NT탐색기와는 현저하게 다르다.

파일과 등록부에 대한 권한화면은 그림 13-5에 보여 준다. 우의 창문은 접근이 보증된 봉사기들을, 가운데창문은 사용자접근이 보증된 등록부들을 그리고 화면의 아래부분에서는 선택된 등록부에 대하여 사용자에게 부여한 권한들을 보여 준다. NetWare등록부의 매 권한들에 대하여 표 13-1에서 설명한다.

표 13-1　　등록부권한들

권한	설　　명
관리자	모든 접근권한을 제공한다.
읽기	사용자가 파일실행 또는 파일내용을 볼수 있다.
쓰기	사용자가 파일내용을 보고 수정할수 있다.
창조	사용자가 새 파일을 창조하거나 지워 진 파일을 되살릴수 있다.
지우기	사용자가 파일을 지우거나 겹쳐쓰기할수 있다.
파일주사	사용자가 등록부안의 파일내용은 보지 못하지만 등록부안의 내용은 볼수 있다.
접근조종	다른 사용자의 위탁배당을 변경시키거나 다른 사용자의 접근권한을 보증할수 있다.

주　　의

창조권한을 가진 사용자는 등록부로 파일복사는 할수 있지만 일단 복사가 된 다음에는 이 파일들을 보거나 수정할수는 없다.

경　　고

관리자권한과 접근조종권한의 할당은 주의하여야 한다. 관리자권한은 완전한 허가를 할당할수 없을뿐아니라 부분등록부에서 려과하여 제거할수도 없다. 그리고 접근조종권한은 사용자가 자기자체가 가지지 못한 허가도 보증할수 있게 한다.

사용자 C가 등록부 A에 대한 파일주사와 접근조종권한을 가졌다고 하자. C는 자기는 읽기, 쓰기, 지우기권한을 가지지 못했지만 사용자 R에게 등록부A에 대한 읽기, 쓰기, 지우기권한을 할당하기 위하여 접근조종권한을 리용할수 있다. 사실 C는 R에게 접근조종권한을 줌으로써 R가 반대로 c에게 완전한 허가설정을 하도록 할수도 있다. 유일하게 제외되는 권한은 관리자에 의해서만 부여되는 관리자권한이다.

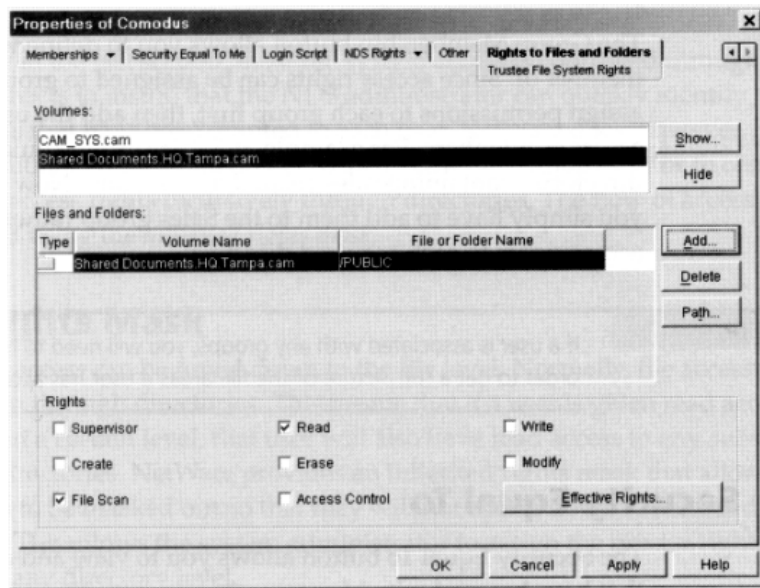



그림 13-5. 파일과 등록부권한화면

그룹성원

그룹성원단추에서는 사용자가 어느 그룹의 성원인가를 정의한다. 접근조종권한이 그룹에 배당할 때 보통 먼저 매 그룹에 권한을 할당하고 다음에 해당한 접근을 요구하는 사용자들을 성원으로서 그룹에 추가한다. 실례로 Sales그룹에 판매관련정보가 있는 모든 등록부들에 접근할수 있도록 허용한다. 그다음 새로운 사용자들이 창조될 때 요구하는 등록부들에 접근권한을 배당하기보다 단순히 Sales그룹의 성원으로 소속시킨다.

일러두기

그룹들과 결합되여 있는 사용자가 접근하는 파일범위는 그룹권한들을 조사하여 알수 있다.

보안등가

보안등가단추에서는 다른 사용자 또는 그룹으로부터 상속된 모든 접근권한을 보거나 또는 구성할수 있다. 이러한 기능을 리용하여 NDS관리자는 모든 보안관련문제를 집중적으로 관리할수 있다.

실례로 모든 보조담당자들에게는 NDS관리자와 등가인 권한을 할당하여 보조담당자들이 자기의 NDS대상들을 관리하도록 한다. 관리자가 사용자별로 검토할 필요가 있는 경우 관리자구좌로부터 각이한 구좌를 보조담당자에게 할당하는것은 자주 쓰는 방법이다. 이렇게 함으로써 경과기록정보를 분할하여 관리한다. 그러나 이러한 관리방법이 경우에 따라서는 불리하다. 그것은 보조인원들이 자기자체의 구좌를 가지고 경과기록를 수정할수 있기때문이다.

그러므로 보조인원들에게는 두가지 구좌를 제공하여야 한다. 하나는 관리자준위의 변경을 할수 있는 구좌이고 다른 하나는 매일 자기의 직능수행을 위한 구좌이다. 관리자가 체계에서 작업할 때 쉽게 해이될수 있다. 유감스럽게도 이러한 부주의는 착오를 가져올수 있다. 완전한 체계접근을 할수 있는 사용자가 소홀히 한탓에 착오를 범할수 있다(F구동기의 파일을 모두 지워 버렸다. F를 플로피디스크로 생각하고…).

관리자기능을 수행할수 있는 후보구좌를 리용하여 보조자가 각성할수 있는 기회를 주고 더 정확히 과제에 전념하게 할수 있다. 요구한 과제를 완성한 보조인원들은 관리자기능을 할수 있는 후보구좌를 반환하고 다시 자기의 사용자구좌를 리용한다.

파일체계

대다수 파일체계접근은 nwadmn95를 통하여 조종된다. 이것은 NDS관리자가 매개 사용자들에 대해 보증한 접근권한을 신속히 식별할수 있게 한다.

NetWare는 려과기라고 부르는 도구프로그람을 추가적으로 제공한다. 이 프로그람은 관리자가 등록부들에 대하여 반복되는 접근권한흐름을 조종할수 있게 한다. 접근권한흐름은 계승권한마스크를 리용하여 조종된다.

계승권한마스크

파일체계접근은 파일준위로 조종할수도 있다. 보통 파일접근권한은 등록부를 기준으로 아래방향으로 유효하게 되여 있다. 이것은 사용자가 특정등록부에 접근할수 있다면 그 등록부안의 모든 부분등록부들에도 접근할수 있다는것을 의미한다. NetWare는 이러한 권한을 마스크시켜 부분등록부에 대한 접근을 금지시킬수 있는 계승권한마스크를 제공한다. 이러한 계승권한마스크를 리용하여 체계관리자는 개별적인 등록부단위로 구체적으로 권한을 할당할수 있다.

실례로 그림 13-6의 등록부구조를 보자. CAM_SYS의 뿌리아래에는 Shared라는 등록부가 있다. Shared등록부에는 부서단위로 여러개의 부분등록부들이 있다. 이때 사용자에게 부분등록부의 내용을 볼수 있게 Shared등록부안에서 파일주사권한을 부여하려고 하지만 Shared등록부내의 모든 부분등록부들에 대해서는 허용하지 않도록 할수도 있다.

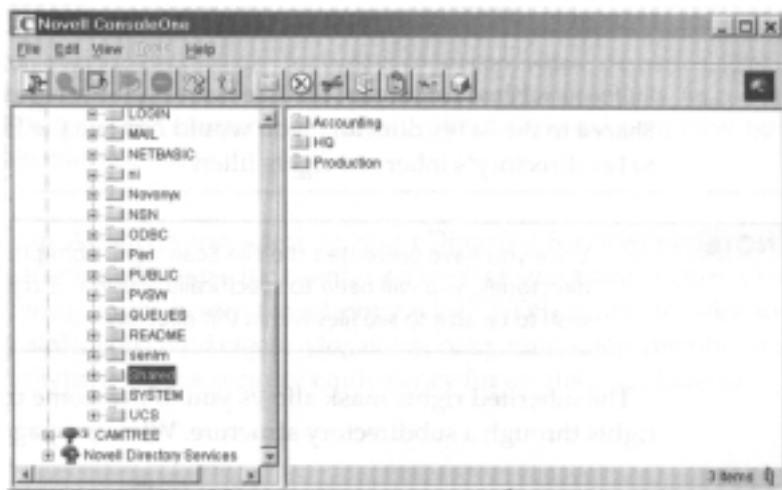



그림 13-6. 등록부구조의 실례

기정으로는 Shared등록부에 대한 파일스캔권한을 가진 사용자는 자동적으로 Sales와 Marketing등록부에 대한 파일스캔권한도 가지게 된다. 이것은 계승권한마스크가 파일스캔권한의 등록부아래방향으로 유효로 되여 있기때문이다. 파일스캔권한을 제거하여 명백히 허가하지 않은 등록부의 내용보기를 제한할수 있다.

계승권한마스크는 Console One에서 해당한 등록부지정, 마우스오른쪽찰각, 속성선택을 한 다음 속성창문(그림 13-7)에서 계승권한려파칸에서 설정한다.

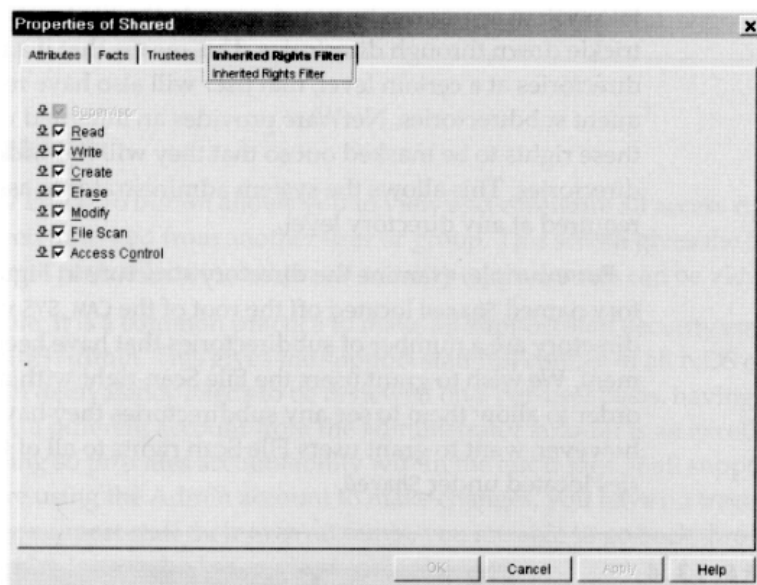



그림 13-7. 등록부의 려과기능설정

만일 Shared등록부로부터 Sales등록부에로 인계되는 파일스캔권한을 무효로 하려면 Sales등록부의 계승권한려과에서 파일스캔권한을 제거하면 된다.

주 의

파일스캔권한의 부분등록부전파를 제한하였으므로 사용자들에게 부분등록부내의 파일들을 볼수 있도록 허가하려면 일일이 파일스캔권한을 부여하여야 한다.

계승권한마스크는 부분등록부로 접근권한이 전파되는것을 무효화시킬수 있다. 일반적으로는 전파가 허용된다. 그러나 관리자는 계승권한마스크를 리용하여 매 등록부들에 대한 접근권한을 구체적으로 할당할수 있다.

경과기록과 검열

NetWare에는 여러가지 류형의 경과기록이 있다. 보안을 위하여 제일 중요한것은 도구프로그람 console.nlm에 의하여 창조되는 조종탁경과기록이다. 이 프로그람은 모든 조종탁동작들과 오유통보문들을 기록한다. 두번째 류형은Auditcon도구프로그람에 의하여 창조되는 검열경과기록이다.

주 의

모든 ABENDS기록은 NetWare봉사기의 SYSTEM등록부안에 있는 abend.log파일에 등록된다. 이 기록정보는 체계를 파괴하려는 해커의 DoS(봉사거부)공격시도를 알아내는데서 매우 중요하다.

Auditcon

NetWare에는 Novell의 체계검열도구프로그람인 Auditcon이 있다. 체계관리자 또는 체계관리자가 지정한 사용자들은 Auditcon을 리용하여 봉사기사건들을 감시할수 있다. 감시할수 있는 사건들은 사용자가입, 통과암호변경, 특정파일접근 등을 포함하여 70개이상이다.

nwadmn 95와 분리되여 존재하는 Auditcon의 우점은 관리자가 사건을 감시하는 사용자를 선발할수 있다는것이다.

일러두기

망관리와 보안감시를 따로 하는 큰 규모의 망에서Auditcon은 아주 쓸모 있다. 이 경우에 감시자는 관리권한이 없이 체계사건을 감시하는데 필요한 권한만을 가진다.

Auditcon을 기동하고 Audit등록부봉사를 선택하여 등록부에 대한 특정사건 또는 사용자가입이름을 검열할수 있다. 그림 13-8은 NDS사건선택화면의 구성을 보여 준다. 실례로 새로운 성원이 그룹에 추가될 때 또는 대상의 보안관련설정이 변경될 때 새로운 기록입구점이 창조되도록 할수 있다.

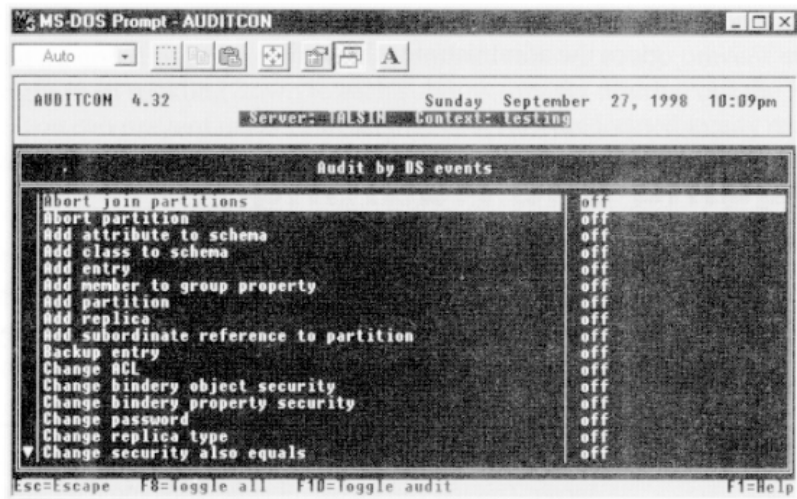



그림 13-8. Auditcon의 ds사건조사화면

특정사용자에 대한 추적은 매우 중요하다. 실례로 관리자준위의 구좌에 의하여 수행된 모든 동작을 기록하여 접근권한이 악용되고 있는가 또는 양도되였는가를 식별할수 있다.

또한 Auditcon을 리용하여 특정한 파일체계의 조작을 검열할수 있다. 실례로 그림 13-9에서는 등록부지우기에 대한 검열을 유효로 설정하고 있다. 또한 특정사용자 또는 사용자일반에 대하여 등록부지우기를 추적할수도 있다.

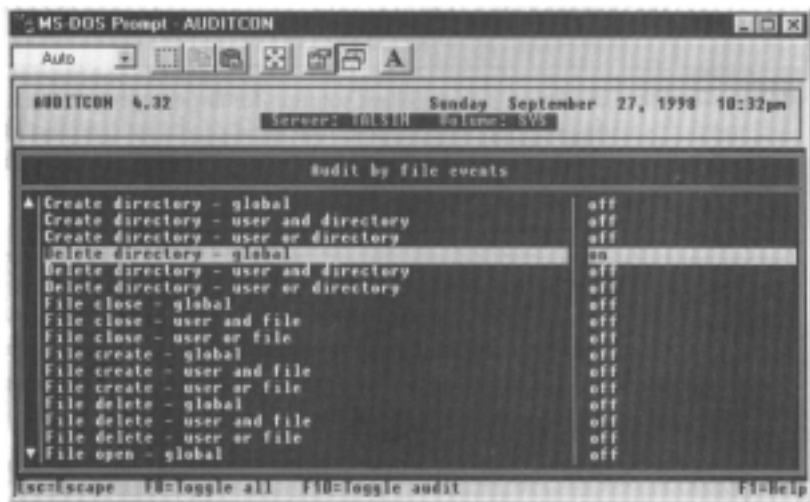



그림 13-9. Auditcon의 특정한 파일사건검열

일러두기

파일체계조작의 추적은 특정파일에 대한 부정호출을 문서화하려는 경우 아주 효과적이다.

망 보 안

NetWare는 망통신의 안전을 위한 여러가지 방법들을 제공한다. 여기에는 NetWare봉사기와의 안전한 통신을 보장하는 파케트서명방법과 파케트려과방법이 있다. NetWare5.0에서부터 Novell회사는 공개열쇠하부구조봉사(PKIS), NDS에로의 LDAP와 SSL의 통합, Novell국제암호화하부구조(NICI), Novell모듈인증봉사(NMAS)와 관련한 기술들을 추가하였다.

파케트서명

수년간 련결가로채기로 알려 진 체계공격의 한가지 류형이 있다. 사용자가 봉사기와 정보를 교환할 때 련결가로채기는 현재 가입한 체계관리자로부터 정보가 오는것처럼 위조한다. 공격자는 봉사기가 접수할수 있는 지령을 보내여 체계관리자로부터 정보가 오고 있는것처럼 속인다.

파케트서명은 이 류형의 공격을 막는데 효과적이다. 파케트서명에서는 봉사기와 워크스테이션이 전송하기전에 서로 약속한 공유열쇠를 리용하여 매 프레임에 서명한다. 이 서명은 동적으로 결정되며 프레임마다 변경된다. 봉사기는 정확히 서명한 프레임을 보내는 워크스테이션이 요구하는 지령만을 접수한다.

공격자가 관리자를 위조하기 위하여 봉사기로 지령을 보내면 봉사기는 유효서명이 없는 수신프레임을 거부하며 그것을 모두 기록한다. 정확한 서명이 부단히 변경되는 경우 어떤 서명이 리용되는가를 알아 내는것은 매우 어렵다. 파케트서명을 리용하면 일상적으로 유지되는 관리자련결을 보호할수 있다.

주 의

파케트서명은 모든 사용자들을 대상으로 할수는 없다.

파케트서명설정

파케트서명은 4개의 보안준위로 구성되며 봉사기와 워크스테이션에서 둘다 설정하여야 한다. 가능한 파케트서명준위들을 표 13-2에서 설명한다.

표 13-2 파케트서명준위

서명준위	설 명
0	파케트서명을 리용하지 않는다.
1	파케트서명을 원격체계가 요구할 때에만 리용한다.
2	파케트서명을 원격체계가 지원하면 리용한다. 그러나 표식은 요구되지 않는다.
3	파케트서명을 지원하지 않는 원격체계와 통신할수 없다.

기정으로 NetWare의뢰기와 봉사기는 1준위로 설정되여 있다. 그러므로 기정설정을 변경하지 않는 환경에서는 파케트서명이 적용되지 않는다.

이동통신연구쎈터(NMRC)는 NT의 C2MYAZZ와 류사한 파케트서명의 속임취약성을 발견하였다. 그것은 공격자가 워크스테이션과 봉사기를 파케트서명을 리용하지 않는것처럼 위조할수 있다는것이다. 이러한 문제는 3준위을 제외한 모든 서명준위들에서 발생한다. 그러므로 망관리자에 의하여 관리되는 모든 워크스테이션들은 반드시 3준위의 파케트서명을 리용하여야 한다.

주 의

NMRC는 Novell제품의 여러가지 취약성을 문서화하였다. 이러한 정보는 Web사이트 www.nmrc.org에서 얻을수 있다.

봉사기에 3준위의 파케트서명을 설정하려면 조종탁에서 다음과 같이 입력한다.

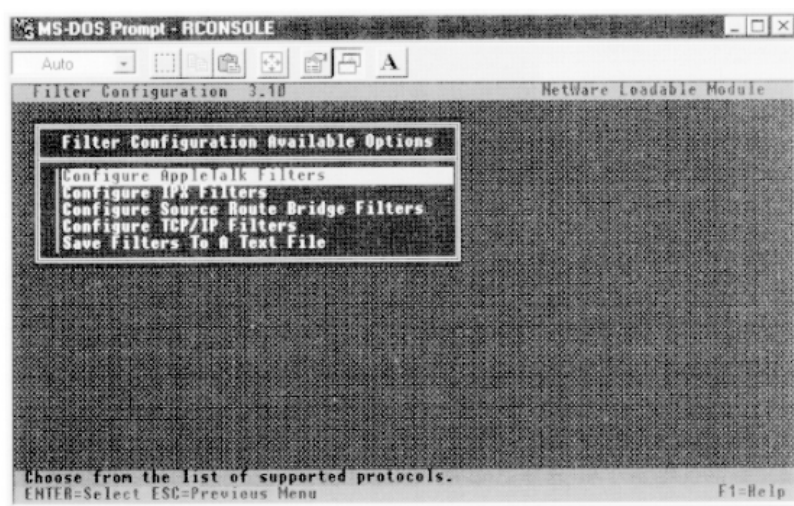
```
SET NCP Packet Signature Option=3
```

의뢰기의 3준위 파케트서명설정은 체계칸(의뢰기를 Windows기반으로 가정한다.)의 N우에서 마우스오른쪽찰칵하고 Novell의뢰기속성을 선택한 다음 설정갱신, 서명준위에서 3을 설정하면 된다.

Filtcfg

NetWare봉사기는 Filtcfg도구프로그람을 리용하여 정적파케트려파기능을 수행한다. 파케트려파기능은 봉사기로 들어 오고 나가는 자료흐름을 조종한다. 만일 2개이상의 망기판을 설치한 경우 파케트려파기능을 리용하여 망토막들사이의 자료흐름을 조종할수 있다. Filtcfg는 IP와 IPx, Appletalk자료흐름에 대한 려파기능을 지원한다.

그림 13-10. 려파기구성차림표

자료흐름을 려파하기 위하여서는 해당 규약에 따르는 Inetcfg도구프로그람을 리용하여야 한다. Filtcfg도구프로그람을 봉사기조종탁에서 적재하여 설치할수 있다. 그림 13-10에 려파기구성차림표화면을 보여 준다. 여기에서 려파규약을 선택할수 있다.

TCP/IP를 선택한다면 려파하려는 경로조종규약을 먼저 밝히고 다음에 려파방향을 지적하여야 한다. 실례로 RIP갱신파케트가 들어 오는것 또는 나가는것을 제거하도록 선택할수 있다. 차이는 봉사기자체가 경로갱신정보를 받아 들이겠는가 하는데 있다. 들어오는 파케트를 려파하면 봉사기에 수신되기전에 제거되므로 갱신이 중단된다. 나가는 파케트를 려파하면 봉사기자체에는 경로갱신정보가 전달되지만 그이후의 다른 망기판으로의 전달은 금지된다.

경로정보를 려파하기 위하여 정적파케트려파기능을 리용할수도 있다. 그림 13-11에 파케트전달려파화면을 보여 준다. Filtcfg는 파케트려파를 정의하는 두가지 방법을 제공한다. 허용하려는 파케트를 규정(기정설정)하든가 또는 거부하려는 파케트를 규정할수 있다. 다른 경우에는 례외를 정의할수도 있다.

그림 13-11. 파케트전달려파화면

실례로 허용하려는 파케트형태를 선택하고 부분망 192.168.1.0과 192.168. 2.0사이에서만 자료흐름이 허용되도록 규정할수 있다. 또한 들어 오고 나가는 모든 FTP련결요구를 거부하도록 례외를 정의할수도 있다. 각이한 려파기능의 조합에 의하여 관리자는 구체적인 접근조종방책을 세울수 있다.

파케트전달려파화면에서 려파기를 지정하고 Enter를 누르면 현재 설치된 려파기목록이 현시된다. 삽입건을 눌러서 려파규칙들을 추가할수 있다. 려파기정의화면을 그림 13-12에 보여 주었다.

원천대면부선택은 려파규칙을 특정한 망기판과 결합시킨다. 이것은 속임려파기를 정의하는데 효과적이다. 실례로 3COM기판으로 NetWare봉사기와 련결된 내부망주소 192.168.1.0이 있다고 하자. 또한 SMC기판으로 비무장지대(DMZ)와 련결되였다고

가정하자. 비무장지대의 파케트들을 막기 위하여 IP원천주소가 192.168.1.0인 SMC대면부에 수신되는 모든 자료흐름을 제거하도록 려과규칙을 정의할수 있다.

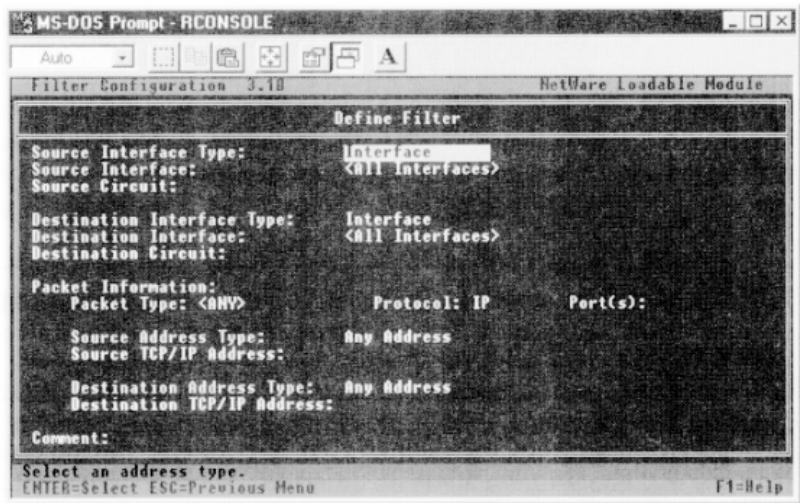



그림 13-12. 려과기정의화면

또한 원천과 목적IP주소, 목적대면부, IP파케트의 류형들도 정의할수 있다. 파케트류형을 지정하고 Enter를 누르면 그림 13-13에서 보여 준 화면이 나타난다. 여기서는 려과규칙을 만드는데 리용할수 있도록 미리 정의된 IP파케트류형목록을 볼수 있다.

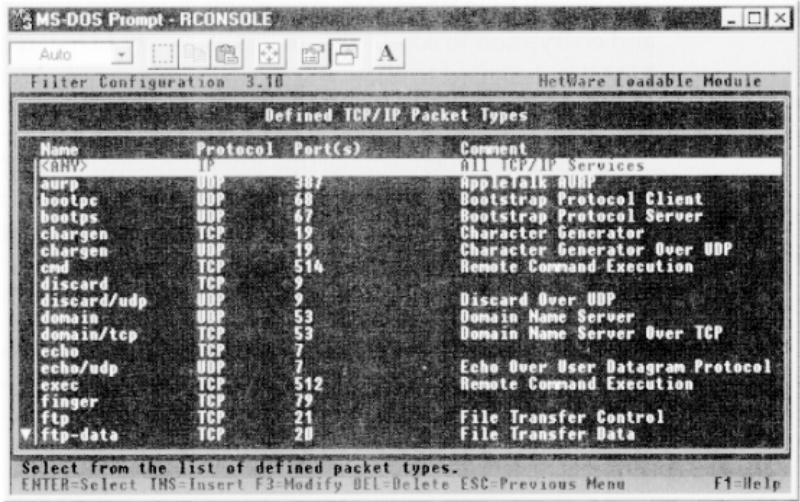



그림 13-13. TCP/IP파케트류형을 정의한 화면

파케트려과기를 정의하는데서는 여러가지 제한이 있다.

• 응답(ACK=1)과 대화설정(SYN=1)파케트를 구별할수 없다.
• ICMP류형의 코드를 정의할수 없다.
• RPC와 같은 동적포구할당을 리용하는 봉사에 대한 지원을 정의할수 없다.

주 의

이러한 제한은 Filtcfg가 명백히 인터네트련결의 안전을 위한 설정항목들을 다 지원하지 못한다는것을 의미한다. 그러나 Filtcfg의 파케트려파능력은 내부망토막들사이 보안을 제공하기에는 충분하다.

려파기규칙을 정의한 다음 탈퇴건으로 정의내용을 보관하고 탈퇴한다. 려파기방책을 유효로 하기 위하여서는 체계를 재기동하여야 한다.

공개열쇠하부구조봉사(PKIS)

Novell은 NDS에서 증서와 열쇠의 요구, 관리, 보관을 위하여 PKIS를 리용한다. 또한 특정한 NDS나무에 고유한(즉 기관에 고유한) 기관적인 증명서권한(ca)을 창조한다. 다른 망들에서 제공하는 보안봉사들은 Novell의 안전인증봉사와 SSL, Novell의 LDAP봉사를 포함하는 PKI에 의거한다. 결과 NetWare봉사기는 인증과 암호화를 리용하여 안전한 가입만을 접수하고 LDAP요구를 확인하며(LDAP는 3자가 주어 진 등록부에 즉 이 경우에는 NDS에 문의할수 있도록 설계되였다는것을 기억하시오.) 망통신을 암호화한다.

여러가지 요소들이 PKI.NLM(NetWare봉사기에서), PKI_SERVER.DLL(NT봉사기에서), LIBPKISERVEc.S와 Npki(Sun Solaris봉사기에서), PKI를 위한 관리도구인 Consoleone을 포함하여 Novell PKI를 형성한다. PKI를 설치한후에 관리상 과제들이 여러개 제기된다.

기관적인 증명서권한(ca)을 창조 이것은 증서와 함께 공개열쇠와 비밀열쇠, 증서고리(허가고리), 기타 구성정보로 구성된다. 비밀열쇠는 암호화되여 NDS에 보관되며 기관적인 증명서권한(CA)은 NDS의 Security등록부에 보관된 대상으로서 표현된다.

봉사기증서대상을 창조 여러 봉사기들의 증서는 하나의 봉사기에 보관될수 있다. PKI형응용프로그람들은 봉사기증서들을 보관한 봉사기에 있는 봉사기증서를 리용하도록 구성된다.

공개열쇠인증을 요구 공개열쇠들은 최소한 공개열쇠, 대상과 발행이름, 유효주기, 계렬번호, 증명서권한의 수자서명을 유지하여야 한다.

Novell의 모듈인증봉사(NMAS)

NMAS는 추가적인 인증기술을 Novell의 견고한 보안체계에 첨부하여 설계되였다. NMAS은 3개의 기본요소 즉 가입인자, 가입방법과 순서, 등급인증을 정의한다. 등급인증은 첫 두개 요소의 결합이다.

가입인자

가입인자는 사용자를 인증하는데 실제로 리용하는 유일한 자료들이다. 가입인자로서 통과암호를 보자. 이것은 사용자만이 실지로 알고 있는것이다. 스마트카드는 사용자만이 가지고 있는것이며 인체정보는 사용자에 해당한 생리학적으로 고유한 정보인것이다. NMAS가 이 3가지인자들을 어떻게 리용하는가를 보자.

통과암호인증 통과암호를 지원하는데는 여러 기술들이 있다. 관리자는 현재의 관리방책 또는 다른 실현기술들과 통합하는 가장 좋은 방법을 리용하기 위하여 다음의 3가지 방안들을 선택할수 있다.

NDS통과암호 사용자이름과 통과암호는 송신되기전에 암호화된다. 이것은 처리기의 속도를 저하시키고 부하를 증가시키지만 안전성은 담보된다.

평문 사용자이름과 통과암호는 암호화되지 않고 평문으로 전송된다. 이것은 관리자가 지정하는대로 낮은 수준의 보안을 실현할수 있다. 전자우편과 같은 일반봉사들에 적용된다.

SMA1/MD5 이 기술은 자료를 망으로 전송하기전에 분할하거나 요약하는 방법으로 정보를 변경한다. 처리는 상대적으로 단순하며 안전은 기본상 담보된다고 볼수 있다.

물리적인 인증 통과암호기술과 같이 사용자의 물리적인 존재를 증명하는데는 여러가지 방법들이 있다. 어떠한 방법을 선택하는가는 보안방책과 현재의 하부구조, 비용 등을 포함한 많은 인자들에 의존한다.

스마트카드 합성수지카드(신용카드와 같은 형태인데 더 두텁다.)에는 수자서명을 포함한 식별정보가 보관되여 있는 프로그람화된 마이크로소편이 내장되여 있다.

통표 손에 건사할수 있는 통표는 사용할 때마다 매번 유일한 통과암호를 발생하는 장치이다. 통표는 보통 다음의 2가지 방법중의 하나에 기초한다.

신청-응답 사용자가 정확한 사용자이름과 통과암호를 제공하면 봉사기가 우연수를 통표와 함께 보낸다. 통표에 보관되여 있는 사용자암호열쇠를 리용하여 봉사기가 보낸 우연수를 암호화하고 다시 봉사기에 반환한다. 사용자암호열쇠의 복사본을 가지고 있는 봉사기는 우연수자체를 암호화하고 결과를 비교한다. 일치하면 사용자가 인증된다.

시간동기 통표와 봉사기는 특정시간내에는 같은 수자를 발생하는 알고리듬을 서로 공유한다. 사용자가 사용자이름과 통과암호를 성공적으로 제공한후에 봉사기는 이 시점에서 통표에 있는 수자를 검사한다. 봉사기가 이 시간내에서 예견한 수자라는것을 확인하면 사용자는 인증된다.

인체정보인증 인체정보인증체계는 식별과 인증을 위하여 측정가능한 생태학적특징을 리용한다. 체계는 여러가지 류형의 수감부와 비교점들 즉 주어 진 대상에 유일하고 특징적인 자료들을 식별하는 쏘프트웨어로 구성한다. 여러 측면에서 비교하여야 하는 인체정보인증체계에서는 사용자를 인증하기 위하여 통계적증명을

리용한다. 이러한 인증체계는 2가지 부류로 나누어 진다.

정적 이 부류의 체계는 시간에 따라 변하지 않은 특징점들에 기초한다. 이러한 특징들로서는 눈의 망막, 지문, 얼굴특징 등이다.

동적 이러한 체계는 사람의 활동과 같은 특징점들에 기초한다. 실례로 음성 또는 필적이다.

방법과 순서

가입방법은 가입인자를 얻는 과정을 의미하며 가입순서는 하나이상의 가입방법들이 있을 때 그 실행순서를 의미한다. NMAS는 가입방법과 순서에 따라서 망자원에 각이한 권한으로 접근할수 있도록 등급인증을 지원한다. NMAS는 방법과 순서를 8가지 등급으로 정의한다. 이 등급을 보안정돈표식이라고도 한다.

- 인체정보, 통과암호, 통표
- 인체정보, 통과암호
- 인체정보, 통표
- 통과암호, 통표
- 인체정보
- 통과암호
- 통표
- 가입(NMAS방법을 리용하지 않고 망접근을 제공한다.)

관리자는 NetWare기록권들에 이 등급들을 할당한다. 사용자가 NMAS를 리용하여 인증되였다면 사용자는 정돈된 대화를 가진다고 말한다. 만일 사용자가 기록권에 할당된 등급과 같은 NMAS등급에 기초하여 인증되였다면 그 기록권에 대한 접근이 가능하며 낮은 NMAS등급에 기초하여 인증되였다면 접근이 불가능하다.

인증방법과 순서가 단순히 통과암호에만 기초하지 않으므로 NMAS는 NetWare의 접근조종을 더욱 강화하고 관리자가 망자원에 대한 접근조종을 강하고 유연하게 실현할수 있게 한다.

NetWare보안의 세부변경

Novell은 봉사기의 보안기능을 더욱 높일수 있는 여러가지 세부변경기능을 제공한다. 여기에는 SECURE. NCF조작과 조종탁파라메터의 여러가지 설정들이 포함된다.

SECURE.NCF

NetWare에는 안전관련규칙을 서술하는 SECURE.NCF파일이 있다. 이 파일은 봉사기가 기동할 때 여러가지 NetWare보호기능들이 자동적으로 유효로 되게 함으로써 봉사기의 보호기능을 높여 준다. SECURE.NCF를 조작하여 다음의 기능들을 수행할수

있다.

- 암호화되지 않는 통과암호의 지원을 무효화
- 일반통과암호를 리용한 조사가능성을 무효화
- 기동시 불량기록권의 자동적인 회복기능 제공
- 불량ncp파케트의 거부

모든 설정들은 대상으로 하는 망체계를 보안상 C2등급으로 실현할 필요가 있는 경우에만 요구된다. C2등급이 요구되지 않는다면 리용하고 싶지 않는 설정들은 주해를 참고하여 선택적으로 조작할수 있다.

보안조종탁

Secure Consol지령이 봉사기조종탁으로부터 기동할 때 다음의 보안기능을 제공한다.

- SYS:SYSTEM등록부에 보관된 쏘프트웨어를 봉사기만이 적재할수 있게 한다.
- 조종탁오유추적도구프로그람을 무효화시킨다.
- 조종탁조작자를 제외한 다른 사람이 시간과 날자를 변경시키는것을 금지시킨다.

Secure console지령이 일단 기동하면 봉사기를 재기동하지 않고서는 무효화시킬수 없다. 안전조종탁의 특징은 봉사기가 조종탁에서 공격을 방어할수 있게 설계되였다는것이다.

원격조종탁접근의 보안

NetWare는 워크스테이션에서 원격에 있는 봉사기조종탁에 접근할수 있게 구성되였다. 접근은 Rconsole도구프로그람 또는 임의의 telnet프로그람을 리용하여 제공된다. 원격조종탁접근시에 발생하는 여러가지 보안상 문제들이 있다. 이러한 취약성은 다음의 단락들에서 상세히 서술한다.

조종탁통과암호의 안전

NetWare 3.2이전 판본들에서는 조종탁통과암호를 AUTOEXEC.NCF에 평문형태로 포함하였다. 그러므로 이 파일에 대한 읽기접근권한을 가진 사용자라면 통과암호를 알수 있다. 봉사기조종탁에 접근하는데 리용되는 통과암호가 secretpass인 경우 지령은 다음과 같다.

load remote secretpass

NetWare 4.1x판본이상부터는 원격접근을 Inetcfg도구프로그람에 의하여 관리한다. Inetcfg의 기본차림표에서 Manage Configration→Configure Remote Access를 선택하여 원격조종탁통과암호를 포함한 모든 원격접근파라메터들을 정의한다.

Inetcfg의 문제는 통과암호정보가 SYS:ETC\netinfo.cfg파일에 평문으로 보관된다는것이다. 이것은 아주 불리하다. 만일 Web 또는 nfs와 같은 IP봉사를 기동하고 있다면 사용자에게는 이 등록부에 대한 읽기접근이 제공된다. 그러므로 임의의 합법적인 체계사용자가 잠재적으로 봉사기조종탁에 접근할수 있게 된다.

따라서 조종탁통과암호의 암호화가 요구된다. 이를 위하여 봉사기조종탁에서 다음의 지령을 실행한다.

load remote <password>
remote encrypt <password>

그림 13-14에서 암호화된 통과암호를 포함하는 파일 SYS:SYSTEM\ LDRE MOTE.NCF의 창조를 보여 준다.

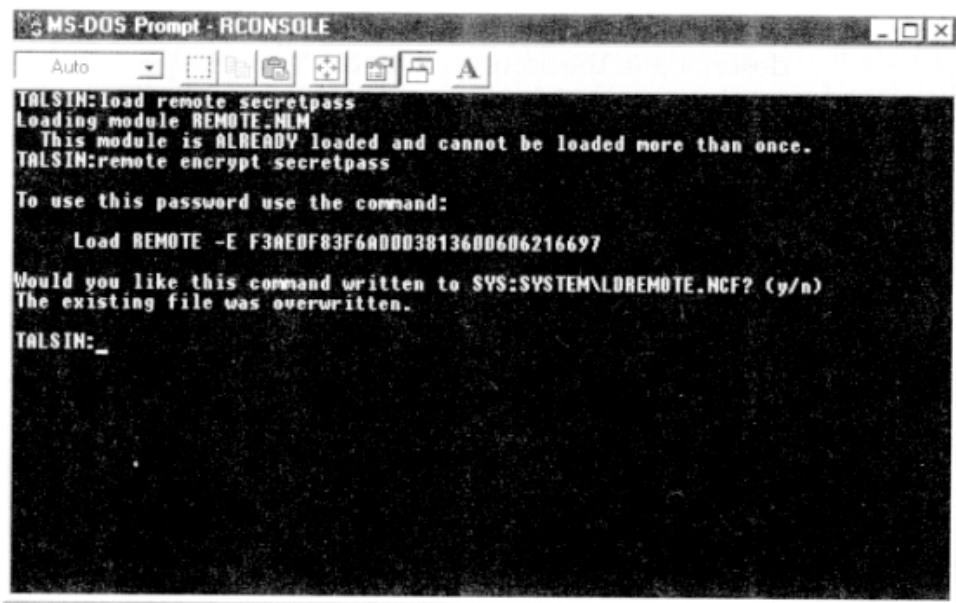



그림 13-14. 원격조종탁통과암호의 암호화

-E스위치는 통과암호가 암호형태로 보관된 원격프로그람이라는것을 나타낸다. 여러가지 선택을 통하여 다음의 기능을 수행할수 있다.

• AUTOEXEC.NCF파일에 있는 INITSYS.NCF조작실행에 앞서 LDREMOTE.NCF 파일을 기동한다.
• AUTOEXEC.NCF파일에 있는 전체 지령을 복사하여 붙일수 있다.
• Inetcfg도구프로그람의 원격접근통과암호마당에 −E스위치와 암호화된 통과암호를 복사하여 붙일수 있다.

일러두기

선택은 자유지만 LDREMOTE.NCF 조작을 리용하는것이 제일 합리적이다. 그것은 SYS:SYSTEM\등록부에 암호화된 통과암호를 보관하고 Inetcfg 의 지령들을 유지할수 있기때문이다.

Telnet를 리용한 조종탁접근

물론 NetWare가 telnet를 리용하여 봉사기조종탁에 접근할수 있는 기능을 제공하지만 그것이 좋은 방법은 아니다. 가장 큰 문제는 telnet대화가 봉사기에 등록되지 않는다는것이다. Rconsole련결은 체계기록정보에 자기 입구점을 가지고 등록되지만 이와는 달리 telnet는 흔적을 남기지 않고 봉사기에 련결된다.

telnet를 기동할 때 다른 문제는 봉사기인증이 평문통과암호를 리용하는것이다. 그러므로 조종탁통과암호를 암호화한다고 하여도 telnet는 그것을 평문으로 전송하기때문에 파케트탐지기를 가진 공격자에게 로출될수 있다.

경 고

Inetcfg도구프로그람은 Rconsole과 telnet지원을 동시에 또는 개별적으로 선택할수 있게 한다. 그러나 telnet지원을 무효로 선택할것을 권고한다.

판도라인자

NetWare봉사기에 대한 매우 성공적인 공격전략은 판도라(Pandora)로 알려 져 있다. 좀더 설명한다면 대등한 공격과는 반대로 설정하여 현재 추진중인 프로젝트와 도구로 되여있는 판도라는 NDS의 결점과 단독봉사기가 아닌 전체 NDS체계에 대한 접근획득을 시도한 NetWare파케트서명의 결함을 리용하였다.

주 의

대다수의 해커도구와 같이 판도라도 자기자체의 보안 특히 사용자통과암호의 강도를 시험해 보려는 합법적망관리자에게 아주 쓸모 있는 도구그룹이다. 참고할수 있는 Web페지주소는 www.nmrc.org/pandora/index.html이다.

판도라방어를 위한 몇가지 단순한 방책들이 있다.

- 판도라는 오직 통과암호가 16문자이하인 경우에만 유효하다. 그러므로 통과암호가 17문자이상인 경우 판도라(현재판)는 무효하다. 관리자통과암호는 적어도 17문자이상 되여야 한다.
- 일부 판도라도구는 NetWare봉사기의 SYSTEM등록부에 대한 접근에 기초한다. 그러므로 관리자만이 이 등록부에 대한 권한을 가지도록 하면 된다.
- 판도라가 감시기를 리용하므로 모든 관리워크스테이션들을 분리시켜서 감시공격으로부터 보호한다.
- 모든 관리워크스테이션들과 봉사기들이 3준위파케트를 리용하도록 구성한다.

요 약

이 장에서는 NetWare봉사기환경을 어떻게 안전하게 하는가에 대하여 고찰하였다. NetWare는 아주 안전한 환경을 제공하지만 망환경을 좀 더 안전하게 하기 위하여서는 몇가지 세부변경이 필요하다. 이 장의 마감에서 구좌관리와 파일접근권한 그리고 NDS조사를 어떻게 진행하는가에 대하여 설명하였다. 또한 왜 원격조종탁에 대한 통과암호의 안전문제가 중요한가에 대하여서도 설명하였다.

다음 장에서는 Windows NT와 NT봉사기의 안전문제에 대하여 고찰한다.

제1 4장. NT와 Windows 2000

Windows NT봉사기는 가장 일반화된 의뢰기-봉사기플래트홈중의 하나이다. Windows 2000은 Microsoft의 제일 중요한 제품인 조작체계의 다음갱신판으로서 보안측면에서 현저한 개선을 실현하였다.

NT봉사기의 보안성은 기정으로는 좀 낮은 수준이다. Windows 2000은 기정구성으로서는 좀 안전하지만 여전히 보안상 부족점을 내포한다. 두 체계의 기정구성의 보안성을 높이는 여러가지 방법들이 있다. 이 장에서는 NT조작체계의 기초적내용으로부터 시작하여 더 안전한 NT환경을 구축하는 방법에 대하여 설명한다. NT와 Windows 2000을 비교하고 Windows 2000의 고유한 보안요구들에 대하여 설명한다.

NT에 대한 개괄

NT봉사기의 기본조작체계는 32bit이다. 16bit Windows응용프로그람들과의 호환성과 같은 일부 문제들이 있지만 이것은 OS을 보다 안전하게 구축할수 있게 한다. NT는 다중과제방식으로 동작하며 다중스레드화가 제공된다. 그러므로 임의의 단일프로쎄스가 CPU사용을 독점하는것을 방지한다.

NT봉사기는 NT워크스테이션과 Windows 95, Windows 98과 같이 32bit Windows응용프로그람 작성대면부를 리용한다. 그러므로 프로그람작성자가 류사한 프로그람작성환경에서 더 안전한 응용프로그람을 만들수 있게 한다. 실례로 Windows탁상응용프로그람을 만드는데 익숙한 프로그람작성자는 Win32대면부를 리용하여 류사하게 NT봉사기에서 프로그람을 만들수 있다. 이것은 NetWare봉사기에서 리용하는 NetWare적재모듈(NLM)과는 대조적이다. NetWare봉사기를 위한 코드를 작성하는 프로그람작성자는 NLM프로그람작성환경을 잘 알아야 한다.

봉사기가 Windows워크스테이션과 같은 Win32대면부를 리용하므로 대부분의 탁상응용프로그람들이 지원된다. 그러므로 체계를 전용봉사기로 리용하지 않는 경우에 아주 편리하다. 체계를 봉사기전용으로 리용하는 NetWare와는 달리 NT봉사기는 사용자워크스테이션으로써도 리용할수 있다. Win32를 지원하는 봉사기는 체계관리자를 위한 실시간절약기라고도 할수 있다. 그것은 탁상기계에서 동작시키는 모든 도구들이 봉사기에서도 동작하기때문이다.

주 의

유감스럽게도 NT는 NetWare의 Rconsole 또는 UNIX의 telnet(telnet봉사기는 Windows 2000봉사기에 포함되여 있다.)와 같은 원격조종기능들은 지원하지 않는다.

Microsoft의 Web싸이트와 그것의 자원들로부터 원격으로 봉사기의 일부 기능을 관리할수 있는 도구들을 얻을수 있으나 규약을 직접 추가하거나 제거, 응용프로그람의 기동, 원격워크스테이션에서 NT봉사기에로의 접근 등은 할수 없다. 이러한 기능을 제공하는데

는 제3자의 쏘프트웨어가 필요하다.

NT는 체계구성정보의 대부분을 보관하기 위하여 등록고라는 자료기지를 리용한다. 이것은 사용자구좌, 봉사, 체계의 장치구동기들일수 있다. 실례로 자료공간 HKEY_USERS에는 사용자구좌와 관련한 정보들이 보관된다. 구성값들을 유지하는 자료공간의 마당들을 열쇠라고 한다.

등록고의 우점은 정보를 집중적으로 보관하고 정보찾기와 변경을 쉽게 한다는데 있다. 거의 모든 NT설정이 도형대면부를 통하여 변경될수 있으며 많은 설정항목들은 등록고안에서 반드시 수동적으로 변경되여야 한다. 등록고의 보기와 변경을 위하여 리용되는 도구는 regedt 32이다.

NT봉사기는 4개까지의 처리기를 지원하는데 하드웨어지원이 있으면 32개까지 증가시킬수 있다. 처리기추가의 우점은 봉사기성능을 향상시킨다는것이다.

가상기억

NT봉사기는 봉사기우에서 동작하는 응용프로그람들이 서로 같은 주기억공간을 리용하지 않도록 분리시키는 기능을 제공한다. 또한 가상기억의 리용도 지원한다. 가상기억은 봉사기가 체계에 설치한 물리적기억보다 더 큰 기억공간을 주기억으로 리용할수 있게 한다. 우점은 응용프로그람이 더 큰 주기억공간을 자유로 리용할수 있다는것이고 부족점은 가상기억이 디스크에 보관된 자료리용을 전제로 하므로 주기억보다 접근시간이 100분의 1정도로 더 느리다는것이다.

가상기억을 리용한다고 하여 주기억공간의 크기를 임의로 줄일수는 없다. 그것은 경우에 따라서 해당한 체계의 정상운영을 담보하는 최소의 주기억공간이 규정되여 있기때문이다. 실례로 Microsoft권고에 의하면 단순히 파일, 인쇄기, HTTP, WINS, DHCP 봉사를 제공하는 봉사기인 경우 최소 주기억공간이 32MB이다. 일부 체계는 원격기동으로 가동한다. 이러한 체계의 성능은 반드시 떨어 진다. 이러한 류형의 체계들에서는 적어도 96～128의 주기억공간이 요구된다.

경 고

등록고에 체계구성정보의 대부분을 포함하고 있기때문에 변경시에 매우 조심하여야 한다. 비상시 리용할 회복디스크를 준비한후에 반드시 등록고를 편집하여야 하며 변경으로 인한 효과를 정확히 리해한 기초우에서 변경을 진행하여야 한다.

NT령역구조

NT봉사기는 사용자와 그룹관리를 위하여 Windows NT등록부봉사를 리용한다. 이것은 이름자체가 의미하는바와 같이 NetWare의 NDS와 같이 완전히 계층화된 등록부봉사는 아니다. 이것은 령역의 리용에 기초한 일반적인 보안구조이다. Windows 2000에서는 NT등록부봉사를 개선하여 능동등록부로 교체하였다. 능동등록부에서는 Windows환경을

계층구조로 관리한다.

령역은 하나의 보안방책에 따라 서로 련결되여 있는 워크스테이션들과 봉사기들로 이루어 진 그룹을 의미한다. 사용자는 한번의 가입으로 령역안에 있는 모든 봉사기들에 대한 접근권한을 얻을수 있다. 즉 매 봉사기에 일일히 가입하여야 할 필요가 없어 진다.

령역정보보관

령역정보는 령역조종기에 보관된다. 매 령역에는 반드시 령역조종기(PDC)가 있다. PDC는 모든 령역정보의 원본을 가지고 있다. 다른 NT봉사기는 2차령역조종기(BDC)로 설정될수 있다. BDC는 PDC로부터 갱신된 정보를 받으므로 령역정보의 복사본을 가지게 된다. 가입하는 사용자는 PDC 또는 BDC에 의해 인증될수 있다.

이러한 구조는 전체 령역모형에서 봉사기가 다소나마 중추적인 역할을 담당하게 한다. 실례로 사용자가 망자원에 접속하기 위한 가입정보를 가지고 있다면 BDC도 이러한 가입정보의 복사본을 가지게 된다. PDC에 있는 가입정보가 변경되면 다른 BDC에도 변경이 진행되여야 한다. 그러나 BDC봉사기의 가입정보는 자동적으로 갱신되지 않는다(즉 PDC에 의하여서만 진행된다.).

일러두기

가입정보를 보안방책의 일부 측면에 국한시켜 리용하지 말아야 한다. 왜냐하면 사용자들이 임의의 시각에 Ctrl+C를 눌러서 가입정보로부터 탈퇴하기때문에 모든 경우를 고려하여 가입정보를 리용하여야 한다.

령역신뢰

계층구조를 모방하기 위하여 령역들이 신뢰관계를 가지도록 구성할수 있다. 하나의 령역이 다른 령역을 신뢰할 때 신뢰된 령역의 사용자들은 자기 령역에서 가지고 있는 접근권한을 그대로 유지할수 있다. 실례로 령역 A가 령역 B를 신뢰한다고 할 때 령역 B에 있는 모든 사용자는 같은 권한으로 령역 A의 자원에 접근할수 있다. 그러나 령역 B가 령역 A를 신뢰하지 않으므로 령역 A에 있는 사용자는 자기의 권한을 유지하며 령역 B의 자원에 접근할수는 없다. 신뢰는 한방향 또는 쌍방향으로 구성할수 있다. 이것을 각각 한방향신뢰, 쌍방향신뢰라고 한다.

령역들사이 신뢰관계를 작은 환경에서 세분화하면 불리하다. 실례로 하나의 콤퓨터에 대하여 령역들사이 신뢰관계를 구성하는것은 망관리에서뿐아니라 망통신에서도 복잡성을 초래한다. 그러므로 함께 작업하는 콤퓨터들을 한번에 매개 령역에 조직적으로 접속하여야 한다. 다른 문제는 여러 령역에 대한 접속을 요구하는 적은 수의 사용자들이 있는 경우이다. NetWare에서는 간단히 접근을 요구하는 등록부들에 가명대상을 창조하면 된다. Windows NT에서는 다중신뢰관계를 창조하지 않으면 불가능하다. 이러한 복잡성을 초래하기보다는 적은 수의 사용자들을 위한 작은 그룹을 새로 창조하는편이 낫다.

신뢰구조설계

신뢰는 보안강화에 리용될수 있다. 한가지 규칙은 단순성을 유지하여야 한다는것이다. 신뢰관계수는 오직 하나 또는 둘로 제한된다. 이것은 신뢰관계가 복잡하게 창조되지 않도록 한다. 또한 관리의 단순성도 보장한다. 그러면 언제 령역신뢰관계가 리용되는가? 그림 14-1에서 그 실례를 보여 준다.

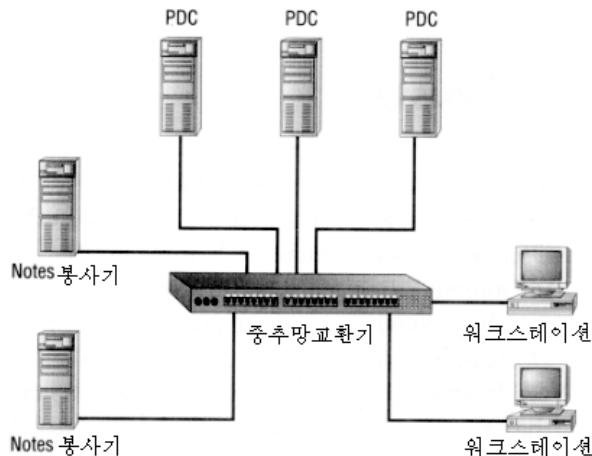



그림 14-1. 령역신뢰가 요구되는 망

이 환경에서는 여러가지 NT PDC와 BDC봉사기가 있다. 또한 Windows NT우에서 동작하는 여러개의 Lotus Notes봉사기도 있다. 망은 2개의 그룹으로 관리된다. 하나는 자료기지, 전자우편 등 모든 Lotus Notes동작을 담당하며 다른 하나는 모든 망기능을 담당한다.

문제는 Notes그룹이 전체 망에 대한 접근을 관리하지 못하도록 하여야 한다는것이다. 이러한 문제는 Notes그룹의 성원들이 불필요한 망자원접근을 하지 않는다는것을 담보하여야 하는 경우에 발생한다. Notes그룹의 성원들은 자기직능을 수행하기 위하여서는 완전한 관리자권한이 보증될것을 요구한다. Notes봉사기에 대한 완전한 관리자권한을 가지지 못하면 체계를 정확히 관리할수 없다.

방도는 2개의 Notes봉사기를 자기령역에 대한 PDC와 BDC로 하는것이다. 이러한 2차령역은 본래의 1차령역을 신뢰하도록 구성할수 있다. 령역구성을 그림 14-2에 보여 준다. 신뢰관계는 Notes그룹이 망의 다른 부분에 대하여서는 관리자준위접근을 가지지 못하지만 2개의 Notes봉사기에 대하여서는 관리자준위접근이 보증되도록 구성되여 있다. 이러한 신뢰관계는 또한 1차령역의 관리자들이 관리자준위접근을 2차령역에서도 그대로 유지할수 있게 한다.

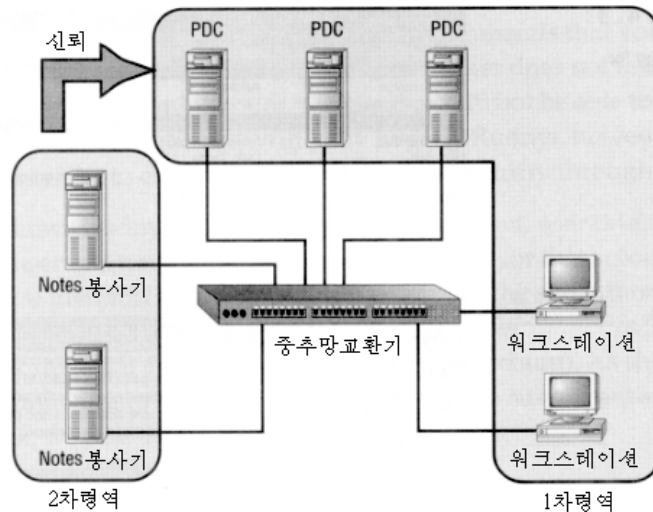



그림 14-2. 신뢰관계

사용자구좌

사용자구좌는 관리도구프로그람그룹에 있는 사용자관리자도구프로그람에 의해 관리된다. 사용자관리자도구프로그람을 그림 14-3에 보여 준다. 여기에서는 사용자추가 및 삭제, 그룹배당, 구좌방책정의를 할수 있다.

모든 사용자접근속성은 파일과 등록부, 공유허가를 제외하고는 이 대면부를 통하여 관리된다. 파일체계허가는 Windows NT탐색기에서 설정한다.

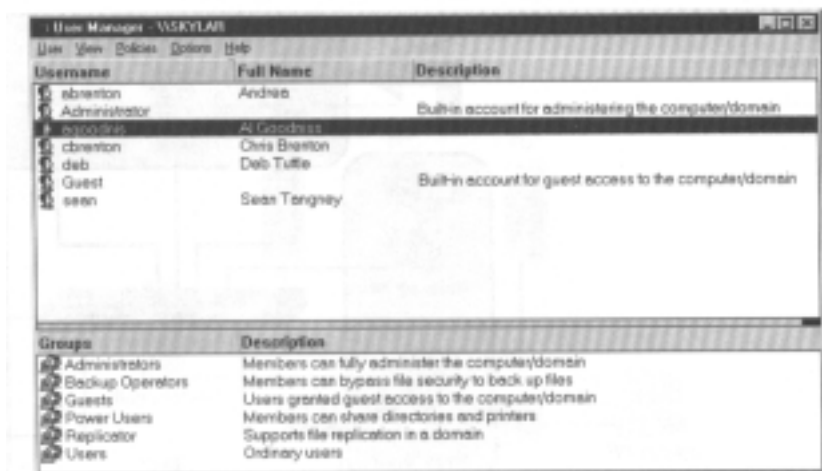



그림 14-3. 사용자관리자도구프로그람

사용자관리자도구프로그람에서는 국부구좌와 령역구좌를 둘 다 관리할수 있다. NT 봉사기와 의뢰기체계는 령역밖에서 관리되는 국부구좌를 가진다. 국부구좌를 NT체계자체가 관리하도록 하기 위하여서는 령역과의 련결을 차단하고 매 체계에 일일이 련결하여야 한다. 국부구좌를 원격으로 관리하려면 사용자관리자도구프로그람에서 User→Select Domain을 선택하고 령역이름대신에 체계이름을 입력시킨다.

일러두기

다중NT체계에서 국부관리자 통과암호를 변경시키면 아주 시끄러운 문제들이 발생한다. Group23이 이 과제를 자동화하기 위한 Perl스크립트를 만들었다. 스크립트는 www.emruz.com/g23/.에서 찾을수 있다.

SID와 관련한 작업

보안식별자(SID)는 매 사용자와 그룹에 배당한 유일한 식별번호이다. SID의 형태는 다음과 같다.

S-Revision Level-Identifier Authority-Subauthority

초기의 S는 이 번호가 SID임을 나타낸다. 부분권한을 제외하고 모든 값들은 령역안의 매 사용자와 그룹에 대하여서는 같다. 부분권한은 사용자와 그룹들사이를 구별하는 유일한 번호를 제공한다. 잘 알려 진 SID에는 여러개의 부분권한번호들이 있다. 이것은 부분권한번호가 매 NT령역안에서는 일관성이 유지되기때문이다. 실례로 관리자구좌는 항상 부분권한값이 500이다. 이러한 정보는 공격자들이 목적구좌를 얻는데 리용될수 있다.

주 의

Microsoft지식문서 Q163846에는 관련구좌들에 따라 모든 SID번호가 목록화되여 있다.

잘 알려 진 SID의 불법리용

Microsoft와 많은 보안전문가들은 NT관리자구좌의 이름을 바꿀것을 권고한다. 론리적으로 공격자는 관리자가 리용하는 가입이름을 모르면 관리자구좌를 얻을수 없게 되여 있다. 그러나 Exgenii Rudny가 만든 도구프로그람들은 애매한 보안시도를 얼마나 쉽게 우회할수 있는가 하는것을 보여 준다.

그림 14-4는 Rudnyi의 2개의 도구프로그람들의 리용을 보여 준다. 먼저 user2sid는 사용자 또는 그룹이름에 기초하여 이 구좌에 대한 SID를 얻어 낸다.

이미 설명한바와 같이 SID는 부분권한열쇠를 제외하고는 모든 구좌에 대하여 같다. 다음에 SID번호(관리자구좌인 경우 500)를 리용하여 목적하는 구좌를 찾을수 있다. 그림 14-4에서 보여 준바와 같이 관리자구좌가 Admin-renamed로 이름이 바뀌였다. 신속히 검사하여 이 구좌가 목적하는 관리자구좌임을 알수 있다.

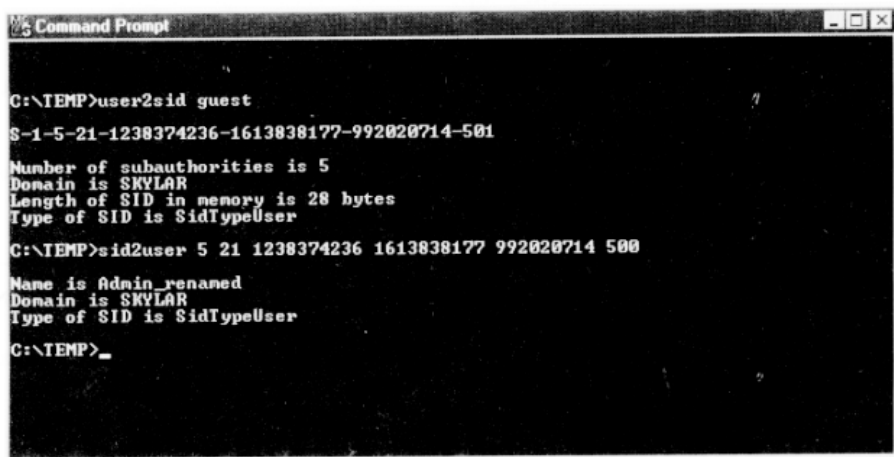



그림 14-4. User2sid와 sid2user 도구프로그람

주　의

Rudnyi의 SID도구프로그람은 www.ntbugtraq.com에서 내리적재할수 있다.

일러두기

관리자구좌의 이름변경은 체계보호를 다소나마 지원한다. 더 좋은 방법은 관리자구좌가 견고한 통과암호를 리용하도록 하며 실패한 모든 가입시도들을 기록해 놓는것이다.

보안구좌관리자

보안구좌관리자(SAM)는 모든 사용자구좌정보가 보관된 자료기지이다. 여기에는 사용자가입이름, SID, 매 통과암호의 암호문들이 포함되여 있다. SAM은 체계보안관리를 책임진 국부보안권한(LSA)에서 리용된다. LSA는 어떤 준위의 접근이 보증되는가를 확인하기 위하여 사용자와 SAM을 결부시킨다.

SAM은 \WinNT\system32\config 등록부에 보관된 파일이다. 조작체계가 항상 이 파일을 열기때문에 사용자는 접근할수 없다. SAM파일은 여러 위치에 놓일수 있지만 관리에서는 주의할 필요가 있다.

\WinNT\repair 이 등록부에는 압축형태로 보관된 SAM파일복사본이 있다. 최소한 관리자와 손님구좌를 위한 입구점을 포함하게 된다.

비상회복디스크 비상회복디스크를 창조할 때 SAM파일이 플로피디스크로 복사된다.

여벌복사테프 NT의 여벌복사프로그람은 SAM파일을 보관할수 있다.

공격자가 이런 3가지 형태로 보관된 SAM파일에 접근할수 있는 경우 체계를 혼란시킬수 있다.

주　　의

16장에서 구좌통과암호를 찾아 내기 위하여 힘내기공격이 어떻게 SAM파일에 가해지는가에 대하여 설명한다.

사용자관리방책구성

NT는 사용자접근방책을 정의할수 있는 여러가지 설정들을 제공한다. 설정들은 2개의 도구프로그람으로 분리된다. 구좌속성과 사용자접근권한은 사용자관리자도구프로그람에서 진행한다. 탁상변경은 사용자관리자에 의하여 진행되지만 방책은 체계방책편집기에 의하여 창조된다.

구좌방책

구좌방책은 사용자관리자에서 Policies→Account선택에서 설정한다. 그림 14-5에서 보여 준 구좌방책창문에서는 체계인증과 관련한 모든 설정들을 할수 있다. 설정은 대역적이다. 즉 모든 체계사용자에게 영향을 준다. 매 선택의 개략적인 설명은 다음과 같다.

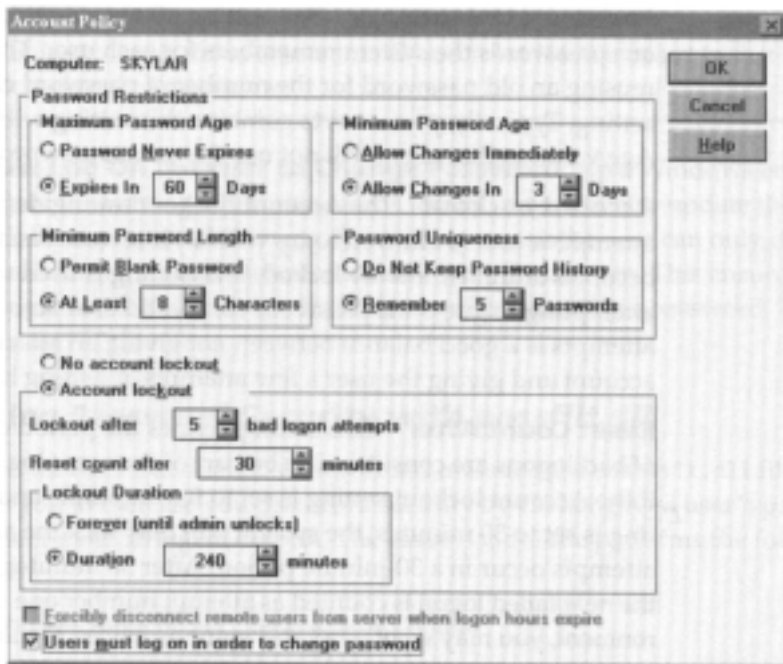



그림 14-5. 구좌방책창문

통과암호의 최대수명 사용자에게 통과암호변경이 강요되기전까지의 시간값을 의미한다. 시간주기가 너무 길면 보안상 위험이 존재하며 너무 짧으면 자주 통과암호를 설정하여야 하는 난점이 있다. 보통 최대 수명은 30～90일로 설정한다.

통과암호의 최소수명 사용자에게 통과암호변경이 허용되기전까지 경과하여야 하는 시간값을 의미한다. 통과암호를 변경시킬 때 일부 사용자들은 통과암호의 유일성을 보장하기 위해서 반복되는 통과암호로 변경을 하려고 한다. 이 선택은 사용자가 과거설정을 취소하든가 또는 현재 값으로 재설정할수 있게 한다. 통과암호의 최소수명을 설정하여 사용자가 같은 통과암호를 다시 리용하는것을 제한할수 있다. 보통 3일부터 7일까지의 값을 설정한다.

통과암호의 최소길이 접수할수 있는 가장 짧은 통과암호의 길이를 의미한다. 16장에서 설명하는 LanMan통과암호의 하위취약성으로 하여 최소길이를 8문자로 할것을 제의하였다.

통과암호의 유일성 체계가 매 사용자에 대하여 이전에 사용한 통과암호를 몇개까지 기억해 두어야 하는가를 지적한다. 이것은 사용자가 통과암호변경시 이 설정값만한 통과암호들에 대하여서는 다시 반복하여 리용할수 없게 한다. 보통 통과암호의 최대수명을 고려하여 같은 통과암호가 1년에 한번이상 다시 리용되지 않도록 설정한다.

구좌차단 이 설정은 사용자가 불법통과암호에 의한 가입시도가 몇번만에 차단되여 구좌가 무효로 되는가를 정의한다. 이 설정은 유효한 사용자구좌를 가지고 통과암호를 추측하려는 공격시도를 막는데 리용된다. 공격자에게 어떤 구좌를 가지고 너무 많이 시도하지 못하도록 그리고 사용자들에게는 자기의 정확한 통과암호를 얻기 위해 몇번의 시도는 허용할수 있도록 균형을 맞추어서 5～6으로 설정한다.

계수재설정 이 설정에서는 불법가입이 다시 반복될수 있는 최소시간주기를 정의한다. 실례로 구좌차단이 5로 설정되고 계수재설정이 30min으로 설정된 경우 체계는 5번 실패한 가입시도가 30min안에 다시 발생하면 구좌를 차단시킨다. 30min후에 계수기는 재설정되며 다음의 첫 가입실패로부터 계수가 시작된다. 환경에 따라서 이 값은 30min으로부터 하루까지 설정된다.

차단지속 만일 구좌가 지나친 가입시도로 하여 차단된 경우 이 설정은 구좌차단이 얼마동안 지속되는가를 정의한다. 고도의 보안이 요구되는 망에서는 이 설정이 무한대이다. 이것은 구좌가 체계관리자에 의하여 재설정될 때까지 차단된다는것을 의미한다. 이 설정기능은 관리자가 구좌차단이 침입자에 의한것인가 또는 자기통과암호를 잊어 먹는 사용자에 의한것인가를 검열할수 있게 한다. 많은 환경들에서 차단설정은 규정된 시간주기후에는 구좌가 유효로 되도록 되여 있다. 이것은 사용자가 자기구좌를 차단시킨 경우 관리자가 그 차단원인을 해명하는데 유효하다. 또한 DoS공격을 막는데도 효과적이다. 어떤 공격자들은 합법적인 사용자들을 차단하기 위하여 의도적으로 불법통과암호를 리용하여 다중가입을 시도한다. 지속설정에 의하여 관리자개입없이 구좌가 유효로 되게 할수 있다.

원격사용자련결의 강제해방 시간제한이 리용될 때 이 설정은 제한시간이 만기될 때는 탈퇴하지 않은 모든 사용자들의 련결을 끊어 버린다. 이것은 사용자가 작업시간후에는 계속 가입을 유지하지 못하도록 함으로써 공격자에게 작업할수 있는 유효구좌가 부여되지 않도록 하는데 유효하다.

일러두기

이 설정은 또한 모든 문서파일을 닫아서 적당한 여벌복사처리가 진행되도록 하는데서도 유효하다.

사용자가 통과암호를 변경하기 위하여서는 가입하여야 한다 Windows환경에서 사용자는 자기의 통과암호를 국부적으로 변경하고 후에 변경사항을 봉사기로 보낼수 있다. 이 설정은 사용자가 오직 령역에서 인증된 대화가 유지될 때만 자기통과암호를 변경할수 있다는것을 의미한다. 이것은 공격자들이 NT령역안의 통과암호를 수정하기 위하여 국부적인 취약성을 리용하지 못하게 한다.

Passfilt.dll에 의한 통과암호 보안의 강화

Microsoft는 Service Pack 2내에 passfilt.dll파일을 후에 추가로 포함하였다. 이 파일은 사용자의 통과암호를 더 엄격한 규범에 맞게 신청하도록 함으로써 통과암호의 보안을 강화할수 있게 한다. Passfilt.dll 파일은 다음의 검사를 수행한다.

- 통과암호는 6개문자이상이여야 한다.
- 통과암호는 대문자와 소문자, 수자, 특수문자(적어도 3종류는 요구된다.)를 혼합하여 만들어야 한다.
- 통과암호는 가입이름 또는 사용자이름의 변종이 될수 없다.

구좌방책은 더 긴 통과암호를 요구할수는 있지만 더 짧게 규정할수 없다. 령역관리자는 이 설정을 사용자별로 제한시킬수는 있다. 이것은 사용자관리에서 특정사용자를 관리하거나 통과암호마당에서 특정통과암호를 설정할수 있게 한다. 이 통과암호는 passfilt.dll에 복종되지 않는다.

Passfilt.dll을 실행하기 위하여서는 등록고열쇠를 입력시킨다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\Notification Packages

다음에 PASSFILT문자렬을 추가한다. 이미 설정된 열쇠값은 지울수 없다.

사용자의 권한

사용자권한은 사용자관리에서 Policies→User Rights를 선택하여 설정한다. 그림 14-6에서 사용자권한방책창문을 보여 준다. 사용자권한은 사용자 또는 그룹이 봉사기에 대

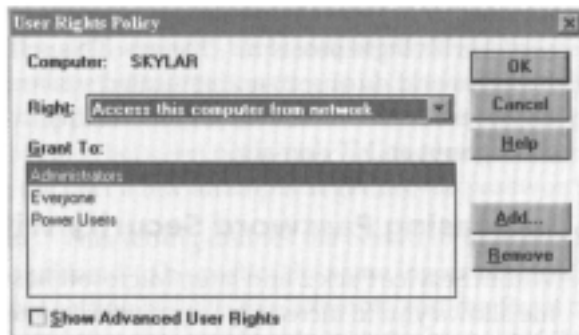



그림 14-6. 사용자권한방책창문

한 특정작용을 수행할수 있게 한다. 권한은 오른쪽 내리펼침차림표에서 선택하고 Grant To칸에서 어느 사용자와 그룹이 이 권한을 보증하는가를 지적한다. Show Advanced User Rights검사에 의해 오른쪽 내리펼침차림표가 추가적인 선택항목을 현시하도록 한다. 중요한 일부 권한들은 다음단락들에서 설정한다.

망으로부터 이 콤퓨터에 접근 이 권한은 령역사용자가 령역안에 있는 매 봉사기들과 원격으로 인증할수 있다는것을 의미한다. 이 권한은 이름봉사기와 같은 특정봉사기를 제외하고 모든 령역봉사기들에 작용한다.

일러두기

관리자의 이름변경대신에 관리자와 동등한 새로운 구좌를 창조하고 이 구좌를 령역관리에 리용할수 있다. 이것은 망으로부터 이 콤퓨터에 접근한다는 권한을 관리자구좌으로부터 제거할수 있게 한다. 관리자는 여전히 망이 아닌 조종탁으로부터 가입할수 있을것이다. 또한 실패한 가입시도를 기록하면 누가 관리자로서 령역에 침입하려고 했는가를 검열할수 있다.

여벌파일과 등록부 이 권한은 모든 파일허가설정을 대신하며 이 권한을 가진 사용자가 전체 파일체계에 대한 읽기접근을 가지게 할수 있다.

경 고

여벌파일과 등록부권한은 위험한 권한이다. 왜냐하면 관리자와 등가라는것을 알림이 없이 전체 체계에 대한 접근을 사용자에게 주기때문이다. 사용자는 이 권한으로 SAM을 복사하고 통과암호크래커를 통하여 체계에 혼란을 조성할수 있게 하는 가능성을 가지게 된다.

우회횡단검사 개선된 사용자권한인 우회횡단검사는 사용자가 설정된 허가준위에 관계없이 파일체계를 검열할수 있게 한다. 파일허가는 여전히 제정되여 있지만 사용자는 등록부들을 자유로 검열할수 있게 된다.

국부가입 령역을 관리할 때 이 권한은 누가 PDC 또는 BDC조종탁으로 가입할수 있는가를 정의한다. 조종탁접근은 관리자준위구좌로 제한되여 있다. 이 설정은 봉사기에 대한 물리적공격을 단념하게 할수 있다. 그러나 완전히 막지는 못한다. 망으로부터 이 콤퓨터에 접근한다는 권한과 같이 이 권한은 불법사용자가 봉사기실에 들어 와서 직접 봉사기에 접근하려고 시도하다가 실패한 가입을 추적할수 있게 한다.

검열과 보안기록관리 파일과 대상검열이 가능할 때 이 권한은 어느 사용자가 보안기록을 검열할수 있는가를 정의하고 어떤 파일과 대상이 검열되여야 하는가를 지정한다.

경 고

누구에게 이 권한을 부여하는가에 대하여 주의하시오. 왜냐하면 공격자가 체계에 침투할 때 흔적을 숨기기 위하여 이 권한을 리용할수 있기때문이다.

보안방책과 프로필

방책은 사용자의 워크스테이션환경기능을 조종할수 있게 한다. 여기에는 조종판의 숨김으로부터 탁상에 없는 프로그람의 기동무효까지 모든것을 포함한다. 방책은 령역에 대하여 대역적으로 설정되거나 또는 특정사용자 또는 그룹에 대하여 설정할수도 있다. 프로필은 사용자의 탁상환경을 요구에 따라서 구성할수 있게 한다. 이것은 특정구좌에 의한 령역인증과 말단사용자에게 탁상환경이 어떤 형식으로 나타나는가 하는 형태로 구성된다. 여기에는 특별한 프로그람그룹 또는 색선택과 화면보호기까지도 포함될수 있다. 프로필을 수행하는데서 여러가지 방법이 있다.

위임프로필 탁상환경이 무조건 적재되는 프로필이다.
위임프로필은 봉사기로부터 적재되며 그 어떤 변경도 허용되지 않는다. 만일 사용자가 탁상환경을 변경하면 다음번의 가입에서 재설정된다.

국부프로필 국부기계에서 적재되며 변경가능한 프로필이다.
사용자가 각이한 워크스테이션으로부터 인증된다면 탁상환경은 다르게 나타난다.

망프로필 배회프로필이라고도 한다. 망프로필은 사용자가 자기의 탁상설정을 임의의 망워크스테이션으로부터 받을수 있게 한다. 망프로필은 위임 또는 변경될수 있는 프로필이다.

방책은 보안방책실현에서 유효하다. 실례로 방책이 사용자가 체계에 쏘프트웨어를 적재할수 없게 되여 있다면 프로필에서 새로운 쏘프트웨어의 설치프로그람을 기동하는데 필요한 도구들을 제거할수 있다. 프로필은 표준탁상을 구성할수 있게 많은 관리도구들을 포함한다.

리용방책

방책은 관리자도구프로그람그룹에 있는 체계방책편집기를 리용하여 창조한다. 그림 14-7에 체계방책편집기를 보여 준다. NT봉사기에서만 다른 NT체계에 적용되는 방책을

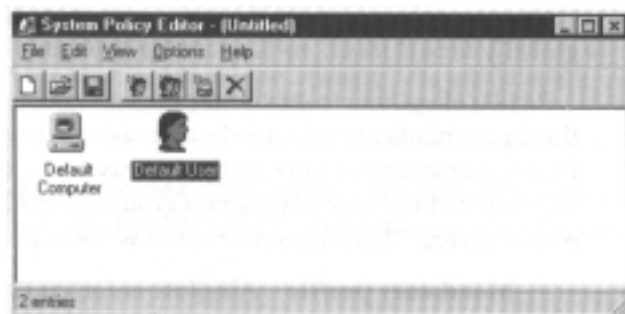



그림 14-7. 체계방책편집기

창조할수 있다. 만일 Windows 95/98체계를 위한 방책을 창조하려고 한다면 WinNT등록부로부터 Windows 95/98콤퓨터로 Poledit.exe파일을 복사하여야 한다. 그다음 Windows 95/98체계에서 방책편집기를 기동하여야 한다.

주 의

방책편집기는 방책을 창조하려는 조작체계우에서 기동하여야 한다.

방책편집기는 사용자워크스테이션환경의 기능을 조종할수 있게 한다. 이것은 체계, 사용자, 사용자그룹에 의해 수행된다. 방책편집기의 기정설정은 모든 체계와 모든 사용자를 위하여 정의되는 방책을 창조할수 있게 되여 있다. 더 큰 환경을 창조하려면 체계와 그룹, 사용자를 추가하는데 Edit차림표를 리용할수 있다.

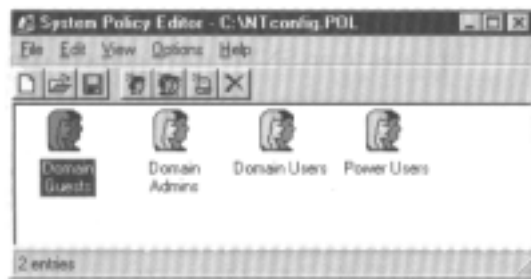



그림 14-8. 단순한 방책

그림 14-8에 보여 준 망은 4개의 그룹으로 구성된다.

- 손님령역
- 관리자령역
- 사용자령역
- 고급사용자

매 그룹들은 자기성원들에게 보증된 접근준위에 기초한 탁상을 형성하도록 할수 있다. 실례로 손님령역은 최소한의 탁상환경을 가지게 하고 관리자령역은 모두 탁상기능들에 접근할수 있게 할수 있다. 사용자령역과 고급사용자그룹에는 손님령역과 관리자령역사이의 탁상기능을 가지도록 할수 있다. 이것은 탁상환경을 여러 준위로 정의할수 있게 한다.

기계방책

기계방책을 구성하기 위하여서는 관리하려는 기계대상을 두번 찰칵한다. 그림 14-9에 콤퓨터속성창문을 보여 준다.

여기서 모든 기계에 대하여(만일 기정방책이 수정된다면) 또는 특정기계에 대하여(Edit→Add Computer를 선택한다면) 실시하려는 방책을 설정할수 있다. 더 유용한 일부 기계방책설정들이 여기에 목록화되여 있다.

그림 14-9. 기정콤퓨터방책을 위한 콤퓨터속성창문

SNMP갱신가능 이 설정은 체계가 SNMP갱신을 SNMP관리조종탁으로 전송할수 있게 한다.

기동 이 설정은 어떤 프로그람들이 체계기동시에 기동하여야 하는가를 결정한다.

공유 이 설정은 관리가능한 공유가 창조될수 있는가를 결정한다.

공유등록부 이 설정은 공유된 프로그람그룹이 체계에 창조될수 있는가를 결정한다.

가입표식 이 설정은 가입설정을 정의한다. 이것은 체계접근을 고려한 공동방책을 보여 주는데 리용할수 있다.

인증창문으로부터 정지 이 설정은 정지선택이 가입인증화면에서 가능한가를 정의한다. 이것은 사용자가 체계에 인증됨이 없이 체계를 정지할수 있게 한다. 기정은 이 선택이 무효이다. 이 칸을 선택함으로써 정지선택을 유효로 한다.

마지막가입이름을 현시하지 않는다 이 선택은 마지막가입이름이 새로운 가입시에 나타나지 않게 한다. 기정으로 Windows는 체계가입을 수행한 마지막사용자를 기억하며 인증창문의 가입이름마당에 현시한다.

사용자와 그룹방책

사용자와 그룹방책을 구성하기 위하여서는 관리하려는 대상을 두번 찰칵한다. 그림 14-10에 보여 준 속성창문이 현시된다. 리용할수 있는 방책설정의 일부는 다음과 같다.

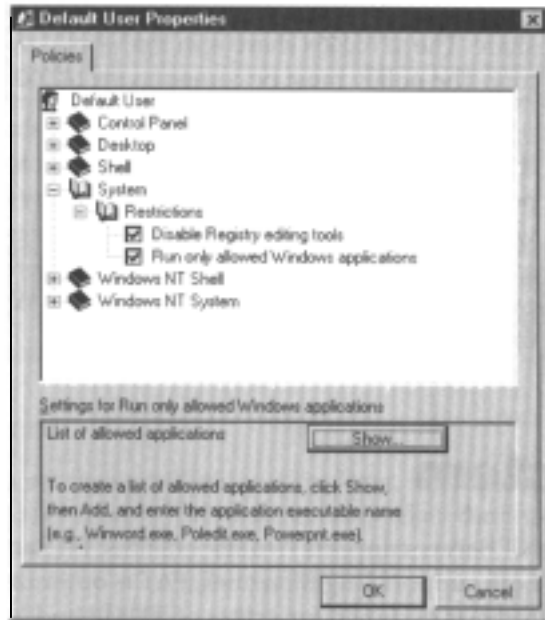



그림 14-10. 기정사용자방책에 대한 속성창문

실행지령제거 사용자가 과제띠에서 Start→Run을 선택하여 지령을 실행하지 못하게 한다.

설정가능성제거 사용자가 Start→Setting을 선택하여 체계구성을 수정하지 못하게 한다.

탐색지령제거 사용자가 Start→Find를 선택하여 국부구동기를 탐색하지 못하게 한다.

나의 콤퓨터에서 구동기숨김 사용자가 나의 콤퓨터그림기호를 리용하여 국부찾기 또는 구동기넘기기를 할수 없게 한다.

망숨김 사용자가 망을 찾지 못하게 한다.

등록고편집도구무효 사용자가 등록고열쇠를 수정하지 못하게 한다.

허용된 Windows응용만 기동 관리자가 사용자가 기동할수 있는 응용프로그람들을 정의할수 있게 한다.

방책유효

방책을 창조한 다음 NETLOGON공유에 보관하면 유효로 된다. NETLOGON공유는 \WinNT\System32\Repl\Import\Seropts등록부에 있다. 방책은 모든 PDC와 BDC의 NETLOGON공유에 복사되여야 한다.

모든 NT체계에 방책을 적용하기 위하여서는 Ntconfig.pol에 방책을 보관하면 된다. 만일 Windows 95/98사용자들에게 적용되는 방책을 창조하였다면 Config.pol로 방책을 보관하고 이 파일을 NETLOGON공유에 복사한다. Windows체계는 령역에서 인증될 때 방책

이 실시되고 있다면 이 특정파일을 찾는다. Windows NT체계는 Ntconfig.pol파일을 찾고 Windows 95/98체계는 Config.pol파일을 찾도록 구성한다.

파 일 체 계

NT봉사기는 2개의 파일체계 즉 FAT와 NT파일체계(NTFS)를 지원한다. 둘 다 긴 파일이름을 지원하지만 FAT는 500MB까지 구동을 위하여 최적화되여 있고 NTFS는 500MB 이상까지 구동하도록 설계되였다. NTFS는 응용프로그람과 사용자파일을 보관하는데 더 우수한 파일체계이다. FAT에서는 지원하지 못하지만 NTFS에서는 파일과 등록부준위의 허가까지 지원한다.

주 의

지워 진 파일의 회복은 오직 FAT파일체계에서만 지원된다. NT는 전적으로 NTFS구동기에서 지운 파일을 회복하는 도구는 지원하지 않는다.

허 가

파일과 등록부에 대하여 2가지 류형의 허가가 있다. 즉 공유허가와 파일허가이다. 공유허가는 사용자가 원격으로 공유된 파일체계에 접근할 때 리용된다. 사용자는 공유허가를 통해서 파일접근을 시도할 때 공유허가는 사용자의 접근이 허용되는가를 검사한다.

파일허가는 파일과 등록부에 직접 할당하는 접근권한이다. 공유허가와는 달리 파일허가는 파일체계에 접근하는데 리용되는 방법을 고려함이 없이 실시된다. 이것은 사용자가 파일체계에 국부적으로 접근한다면 공유허가는 설정되지 않았지만 여전히 파일준위허가에 의하여 접근할수 있다는것을 의미한다.

주 의

이러한 구별은 Web봉사기와 같은 봉사의 허가설정에서 중요하다. Web봉사기에 대한 접근설정은 파일준위허가에 의하여서만 조정된다. 이때 공유허가는 무효하다.

망의 공유자원에 접근할 때 허가는 중첩된다. 이것은 사용자에게 아주 엄격한 준위의 접근을 제공한다는것을 의미한다. 실례로 원격사용자가 완전조종접근권한을 가지고 있다고 하여도 읽기접근만을 허용하는 공유자원에 대해서는 읽기접근만이 가능하다. 그림 14-11에 공유문서속성창문을 보여 준다.

보안이라고 표식한 표적에서는 다음단락에서 설명하는 파일준위허가를 설정한다.

공유문서속성창문에서 허가단추를 설정하면 그림 14-12에 보여 준 공유허가접근창문이 나타난다.

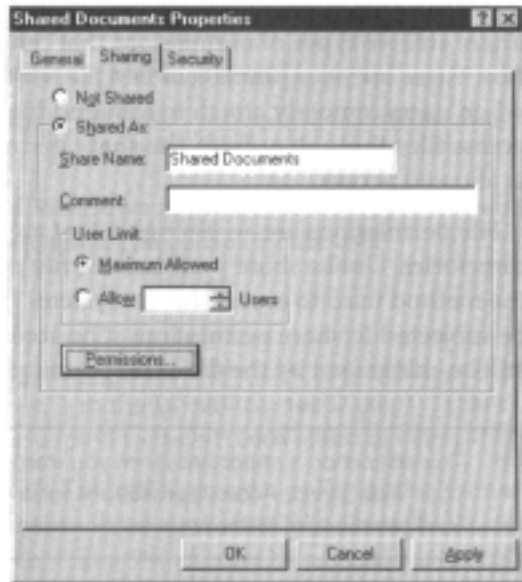



그림 14-11. 공유문서등록부의 공유속성창문

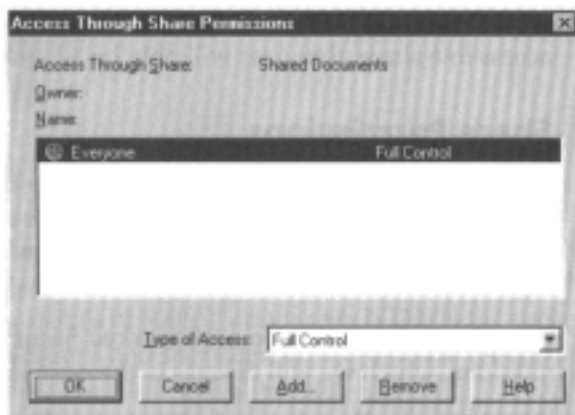



그림 14-12. 공유허가접근창문

기정으로는 모두에게 공유자원에 대한 완전조종접근이 주어 진다.

일러두기

Microsoft의 파일공유는 모두에게 완전접근을 담보한다. 그러므로 공유허가준위를 자주 재검토하고 가능한 접근준위를 제한하여야 한다.

접근준위는 각이한 그룹들 또는 특정사용자들과 어떤 공유허가를 결합하여 설정한다. 이것은 매 사용자 또는 그룹이 특정한 공유자원에 대한 접근을 시도할 때 어떤 준위를 가지는가를 정의한다. 배당할수 있는 공유허가는 오직 4가지 준위이다.

비접근 공유자원에 대한 접근이 허락되지 않는다.

읽기 사용자 또는 그룹은 등록부구조를 검열하여 파일보기, 프로그람실행을 할수 있다.

변경 사용자 또는 그룹은 읽기허가를 가지며 파일과 등록부를 추가, 삭제할수 있다. 허가는 현재 파일이 변경된 경우에도 보증된다.

완전조종 사용자 또는 그룹은 변경허가를 가지며 파일허가를 설정하고 파일과 등록부의 소유권을 가질수 있다.

기정설정보다 더 많은 공유허가설정을 그림 14-13에 보여 준다. 이 구성에서는 기정으로 접근조종목록에 아무도 없으므로 누구도 접근권한을 가지지 못한다. 사용자령역그룹에 속한 사용자에게는 변경준위접근이 허용된다. 관리자령역에는 공유자원에 대한 완전조종이 허용된다. 그러므로 관리자령역이 요구되는 모든 관리기능들을 수행할수 있게 된다.

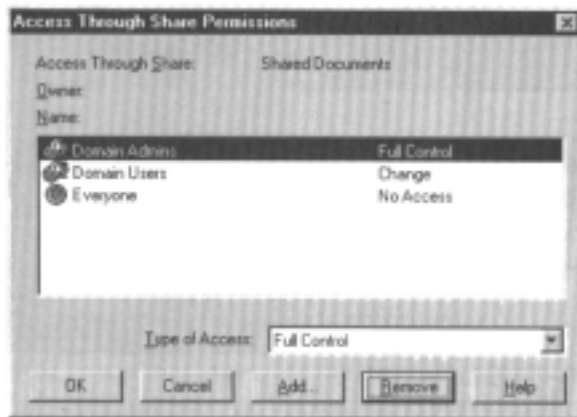



그림 14-13. 제안된 일부 공유허가

일러두기

공유허가를 수정할 때에는 항상 먼저 령역관리자에 대한 허가를 추가하시오. 그것은 령역관리자들이 접근권한을 가지지 못하게 공유자원을 구성할수 있기때문이다.

공유허가를 구성한 다음 변경사항이 보관되도록 OK를 찰칵하시오. 화면을 닫기전에 공유준위를 다시 검사하는 습관을 가지는것이 좋다. 공유허가는 즉시 유효로 되여 이 공유자원에 대한 접근을 요구하는 모든 사용자들에게 접근가능성을 준다.

파일보안

파일허가는 또한 탐색기에서 등록부지정, 오른쪽 찰칵, 속성창문열기를 한 다음 설정할수 있다. 여기서 보안표적을 선택하면 그림 14-14에 보여 준 창문이 나타난다.

창문에는 파일허가와 검열 또는 파일소유권을 조작할수 있는 3개의 단추가 있다.

그림 14-14. 공유문서등록부의 보안표쪽

허가단추

파일과 등록부허가는 허가단추를 선택하여 수정한다. 그림 14-15에 등록부허가창문을 보여 준다. 그림에서 알수 있는바와 같이 파일과 등록부허가조작은 공유허가조작과 거의 류사하다. 차이는 더 많은 선택항목들이 있다는것이다.

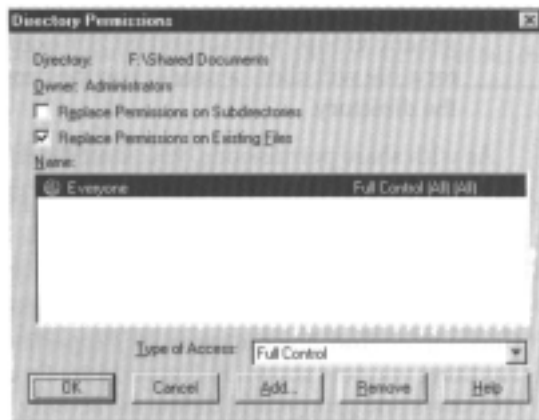



그림 14-15. 등록부허가창문

화면우에 2개의 검사칸이 있다. 공유자원대신에 등록부를 조작하여 체계는 등록부안의 모든 대상들에 적용하려는 보안변경을 진행할수 있다. 만일 현존파일에 대한 허가반환검사칸만이 유효로 되여 있다면 허가는 등록부안의 파일들에만 적용된다. 부분등록부에 대한 허가반환검사칸이 유효이면 등록부안의 파일들과 부분등록부들에로 재귀적으로

허가변경이 적용된다. 두개의 검사칸이 다 무효이면 허가는 등록부에만 적용되고 다른 등록부 또는 파일들에는 적용되지 않는다.

공유허가와 같이 파일 또는 등록부허가는 사용자 또는 그룹과 특정접근준위를 결합하여 설정한다. 등록부허가를 조작할 때 7가지준위의 허가를 설정할수 있다. 이것은 접근허가설정보다 좀더 세분화할수 있게 한다. 허가설정은 다음과 같다.

비접근 등록부접근을 허용하지 않는다.

목록 사용자 또는 그룹이 등록부구조를 검열하고 파일목록은 볼수 있지만 파일접근은 할수 없다.

읽기 사용자 또는 그룹이 목록허가를 가지며 파일보기와 프로그람실행을 할수 있다.

추가 사용자 또는 그룹이 목록허가를 가지며 파일과 등록부를 추가할수 있다. 파일을 보거나 실행시킬수는 없다.

추가와 읽기 추가와 읽기허가를 가지므로 파일을 추가하거나 볼수 있다. 그러나 삭제와 변경은 할수 없다.

변경 사용자 또는 그룹은 추가와 읽기허가를 가지며 파일과 등록부를 지울수 있다. 현존파일을 변경할수도 있다.

완전조종 사용자 또는 그룹은 변경허가를 가지며 파일허가를 설정하고 파일과 등록부의 소유권을 가질수 있다.

특정접근 이 설정은 파일과 등록부에 정확한 권한을 배당하도록 지정할수 있다. 선택은 읽기, 쓰기, 실행, 지우기, 변경허가 또는 소유권얻기이다. 이것은 일반적인 그룹으로 되지 못하여 어떤 하나의 허가만이 요구되는 경우에 효과적이다. 실례로 파일에 대한 실행허가만을 설정하면 사용자는 등록부에 대한 접근을 가지지 못하지만 프로그람을 실행시킬수는 있다.

공유허가와 같은 매 사용자 또는 그룹이 요구하는 최소준위의 접근을 결정하고 허가를 적당히 설정하여야 한다.

검열단추

검열은 봉사기의 파일에 누가 접근하는가를 감시할수 있게 한다. 속성창문에서 검열단추를 찰칵하면 그림 14-16에 보여 준 등록부검열창문이 나타난다. 여기서 특정사용자와 그룹을 등록하고 등록하려는 조작을 정의할수 있다. 실례로 그림 14-16에서는 등록부의 소유권과 허가변경을 검열할수 있다.

이 특성을 리용하기 위하여서는 또한 사용자관리자를 기동하고 Policies→Audit를 선택하여야 한다. 검열이 유효로 되자면 동시에 파일과 대상접근이 허용되도록 설정되여 있어야 한다. 모든 검열입구점들은 사건보기(Event Viewer)에 있는 보안기록에 보고된다.

주 의

검열은 이 장의 《경과기록》에서 구체적으로 설명한다.

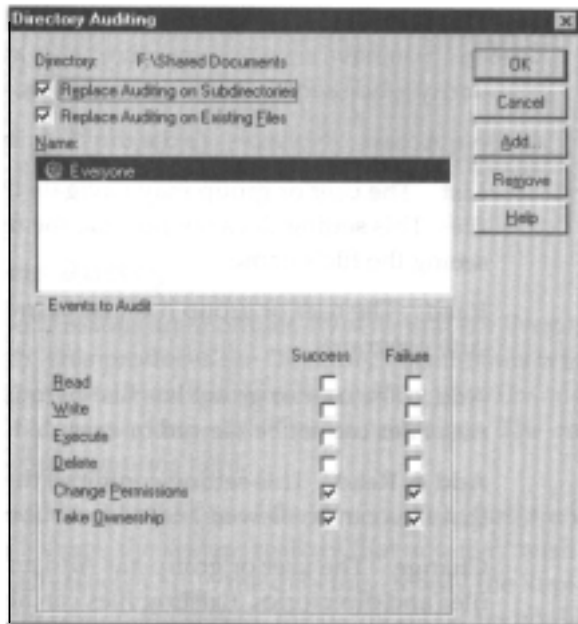



그림 14-16. 등록부검열창문

소유권단추

속성창문에서 소유권단추를 눌러서 파일과 등록부의 소유권을 가지도록 할수 있다. 령역관리자는 항상 소유권(파일 또는 등록부의 완전조종을 가지도록 제공된다.)을 가질수 있다. 만일 완전조종이 사용자령역에 주어 지면 이 사용자들은 소유한 파일과 등록부의 소유권을 가질수 있는 다른 사용자그룹을 선정할수 있다.

경 과 기 록

모든 NT사건들은 사건보기(Event Viewer)를 통하여 보고된다. 사건보기는 관리자도구프로그람그룹에 있다. 기정으로는 체계와 응용프로그람통보문만이 기록된다. 그러나 여러 보안관련사건들을 추적하도록 검열기능을 설정할수 있다. 이것은 체계에서 무엇이 진행되고 있는가 하는 매우 상세한 정보를 제공한다.

사건보기의 구성

사건보기에는 여러가지 설정들이 있다. 기본차림표에서 Log→Log Settings를 선택하면 그림 14-17에 보여 준 사건기록설정창문이 나타난다. 설정변경차림표에서는 체계, 응용프로그람, 보안기록을 개별적으로 구성할수 있다. 기록의 최대크기의 설정뿐아니라 기록정보가 방대해 지면 어떻게 하여야 하는가도 지적할수 있다.

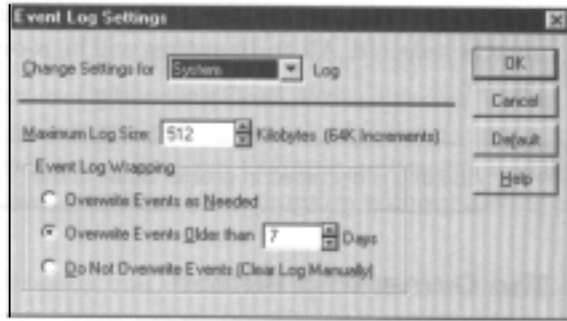



그림 14-17. 사건기록설정창문

일러두기

기정으로 설정되여 있는 512KB기록공간은 너무 작다. 사건보기는 중요한 사건들에 대한 추적정보를 기록한다. 그러므로 기록공간을 충분히 크게 하여야 한다. 3가지 형태의 기록을 모두 보존하기 위하여서는 기록공간의 크기를 4098KB로 확장한다. 기록공간의 최소크기는 12MB이다. 이 경우는 체계자체의 정상운영을 위한 기록정보만이 보관된다.

사건기록의 포장에 대한 기정설정이 또한 문제이다. 체계가 60일이상 기동하다가 파괴된 원인을 검열한다고 할 때 어떤 문제가 생기겠는가? 한주일마다 사건기록정보를 중복하여 보관하였다면 체계파괴원인을 추적하는데 필요한 리력정보가 모두 유지되지 못하였을것이다. 3가지 형태의 기록을 모두 유지하기 위하여서는 사건중복기록금지설정을 유효로 변경한다. 이것은 기록파일이 기록공간을 초과하면 조종탁오유를 발생하지만 사건추적을 위한 리력정보가 분실되는것보다는 유리하다.

사건보기기록의 검사

기록을 정상적으로 검사하도록 규정을 세워야 한다. 이것은 체계에 누가 침입했는가를 추적하는 좋은 방법이다. 기록정보는 관리자가 없을 때 누가 체계에 접근했는가를 보여 준다. 설정에 따라서 기록입구점들을 수동적으로 또는 자동적으로 검사할수 있다.

수동적인 기록검사

기록검사의 제일 단순한 기록검사방법은 반드시 조종탁으로부터 체계에 가입하도록 하고 기록입구점들을 검사하는것이다. 하나 또는 2개의 봉사기가 있는 경우 이 방법이면 충분하다. 경과기록은 사건보기창문에서 Log→Save As를 선택하여 파일로 보관하여 보존한다. 기록정보를 a.TXT파일로 보관하고 Excel과 Access와 같은 다른 프로그람에 의하여 검사하도록 할수 있다. 유연성디스크로 보관할 때에는 먼저 압축을 하게 된다. 12MB의 가치 있는 기록정보를 쉽게 하나의 플로피디스크에 보관할수 있다.

10이상의 NT체계를 관리하는 경우 매 체계에서 검사를 진행하는것은 현실적이 못된다. 사건보기기본차림표에서 Log→Select Computer를 선택하면 그림 14-18에 보여 준 콤

퓨터선택대화칸이 연시된다. 여기에서 Windows NT체계를 선택하고 원격으로 사건보기기록들을 찾아 볼수 있다. 이것은 기록정보를 집중적으로 관리하는데서 효과적이다. 또한 기록정보는 국부적으로 보관되도록 할수 있으며 기록정보에 단일걸음처리를 보존하도록 할수도 있다.

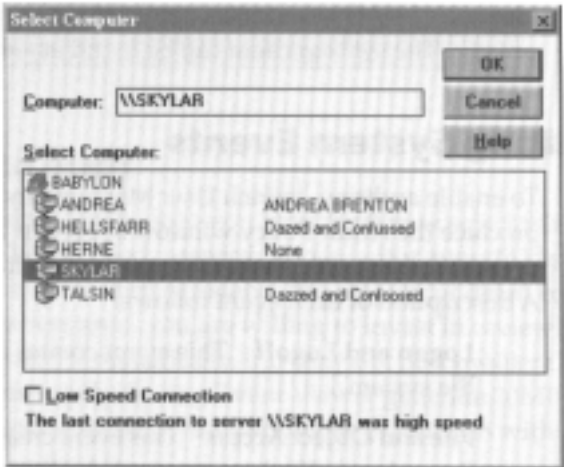



그림 14-18. 콤퓨터선택대화칸

일러두기

탁상체계가 Windows 95/98이면 원격으로 사건보기의 기록정보를 볼수 있다. 이 경우에 Windows 95/98을 위한 NT관리자도구를 얻을 필요가 있다. 이것은 Windows 95/98을 위한 사건보기, 사용자관리자, 봉사기관리자를 포함한 실행가능파일(nexus.exe)이다. 이 도구는 Windows 95/98체계로부터 NT령역을 관리하는데 리용된다. Nexus.exe보존파일은 Microsoft의 Web싸이트에서 얻을수 있다.

자동적인 기록검사

수백 또는 수천개의 NT체계를 관리한다면 모든 사건보기의 기록정보를 수동적으로 검사할수는 없다. 많은 체계를 검사하여야 한다면 그 과정을 자동화할 필요가 있다. 자동적인 기록검사처리는 체계에서 일어 난 상황을 검열하기 위하여 사건보기기록정보를 탐색하도록 한다.

검열하려는 입구점이 발견되면 표식을 하여 검열할 필요가 있다는것을 체계관리자에게 알린다. 자동적인 기록검사처리는 어떤 사건발생을 추적하는데 드는 사람의 작업량을 훨씬 감소시킨다.

검사처리를 자동화하는 제일 안전한 방법은 기록자료를 원격체계로 전송하는것이다. 기록자료들이 전송될 때 공격자들이 흔적을 없애기 위하여 전송자료를 수정하려고 하므로 그것에 대한 보호대책이 필요하다.

Elmar Haag는 NT체계가 자기의 기록자료들을 syslogd가 실행되고 있는 UNIX체계에 전송하는 프로그람을 만들었다. 이것은 기록정보를 통합하여 집중적으로 자동처리할수 있게 한다.

체계사건의 검열

검열을 유효로 하기 위하여서는 사용자관리자를 기동하고 Policies→Audit를 선택하여야 한다. 그림 14-19에 검열방책창문을 보여 준다. 사건목록에서 성공, 실패 또는 둘 다 동시에 기록하겠는가를 선택할수 있다. 검열할수 있는 사건들은 다음과 같다.

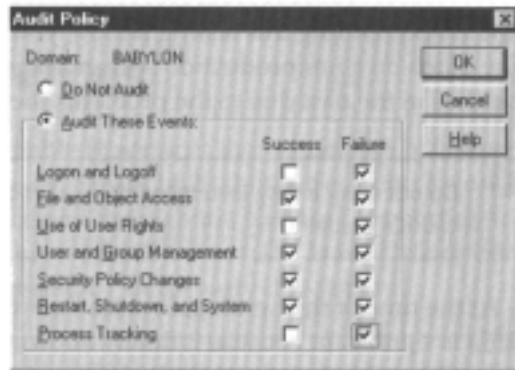



그림 14-19. 검열방책창문

가입과 탈퇴 사용자가 체계에 가입하거나 탈퇴할 때 하나의 기록입구점을 창조한다.

파일과 대상접근 검열되여야 하는 파일과 대상에 접근할 때 기록입구점이 창조된다. 검열은 이 장에서 이미 설명하였다.

사용자권한의 리용 사용자권한이 확인될 때 기록입구점이 창조된다. 이 사건을 선택하면 매우 큰 기록파일이 창조된다.

사용자와 그룹관리 사용자와 그룹이 추가, 삭제, 수정될 때 기록입구점이 창조된다.

보안방책변경 그룹권한 또는 검열사건과 같은 보안방책이 수정될 때 기록입구점이 창조된다.

재기동, 정지, 체계 체계가 재기동하거나 정지될 때 또는 보안기록설정이 변경될 때 기록입구점이 창조된다.

프로쎄스추적 응용프로그람 또는 봉사호출을 추적한다. 이 사건을 선택하면 매우 큰 기록파일이 창조된다.

검열항목결정

검열선정이 유효로 주어 진 경우에는 감시하려는 사건들을 선택하여야 한다. Knee-jerk호상작용은 모든것을 감시한다. 그러나 이것은 실천적이 못된다. 성능측면을 고려하여 기록정보검열에 필요한 시간과 자원을 고려하여 검열항목을 결정하여야 한다. 가령 매일 20MB의 기록정보가 생성되는 체계를 수동적으로 검사한다면 체계추적은 불가능

하다.

해결방도는 극히 중요하다고 생각되는 사건들을 추적할수 있도록 보안방책을 설정하는것이다. 실례로 성공하는 모든 가입사건들에 대해서는 엄밀히 검열할 필요가 없다. 이러한 정보들을 검열한다면 려파하여야 할 기록입구점들을 검사할 필요가 없다. 그러나 실패한 가입사건들에 대하여서는 경우가 다르다. 그것은 공격자들의 첫 시도가 체계접근을 얻는것이기때문이다.

일러두기

기본문제는 기록공간의 크기를 관리할수 있도록 유지하는것이다. 어떤 문제를 검사하는데 다시 리용되지 않는 기록입구점들은 계속 보존할 필요가 없다.

보안림시보수

NT는 지난 몇년동안 보안상 여러가지 취약성으로 해서 손해를 보았다. 매달 2 또는 3건의 주요보안결점들이 드러나고 있는것이 일반적이다. 이런 리유로 해서 안전하다고 생각되는 모든 보안관련수정프로그람들을 리용하는것이 중요하다. 검사주기동안에는 비제품화된 봉사기에서 보안림시보수프로그람들을 검사한다. Microsoft는 지난시기 자기들이 만든 문제점들로 해서 보안림시보수프로그람들을 취소할 필요가 있었다.

경 고

새로운 보안림시보수프로그람들을 문제점이 없다는것을 확인할 때까지 제품화된 봉사기들에 적용해서는 안된다.

이 책이 출판될 당시는 Service Pack 6a가 최신 주요수정프로그람이였다. SP6a는 NT4.0이 C2등급으로 보증되도록 한것으로 하여 중요한 의미를 가진다. C2보증은 국가안전보장국(NSA, National Security Agency)산하인 국가콤퓨터보안쎈터 (NCSC)에 의하여 진행된다. C2보증을 위하여서는 다음의 보안특성들이 요구된다.

위임사용자식별과 인증 확인된 사용자를 식별하고 그들에게만 체계자원접근을 허용하도록 할수 있는 체계의 능력
선정가능한 접근조종 사용자들은 자기들의 요구에 맞게 정보를 보호할수 있다.
검열과 구좌 모든 사용자들의 자원접근을 추적하고 기록한다.
대상재리용 이미 리용된 자원에 대한 사용자접근을 막을수 있는 조작체계의 능력

MSA는 C2보증을 위하여 다음의 절차들을 리용하였다.

- 원천코드의 검사
- 세부설계문서의 검사
- 평가에서 나타나는 오유들이 수정되였는가를 확인하는 재검사

일러두기

IIS를 기동하고 있다면 설치할수 있는 여러가지 다른 보안림시보수프로그람들을 얻을수 있다. Microsoft Web싸이트에서 최신보안림시보수프로그람목록을 보시오.

리용가능한 IP봉사

이 단락에서는 NT봉사기에서 리용가능한 IP봉사들을 요점적으로 설명한다. NT봉사기에서 리용가능한 IP봉사들이 목록화되여 있는 봉사추가차림표를 그림 14-20에 보여 준다. 디스크에 의한 선택단추는 제3자의 개발자가 만든 IP봉사를 추가할 때 리용한다.

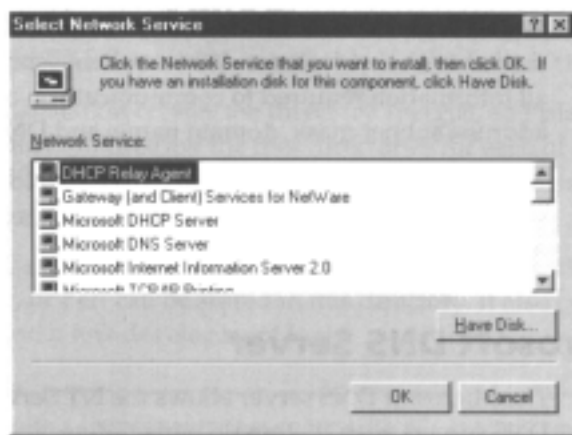



그림 14-20. NT봉사기에서 봉사추가차림표

콤퓨터열람기

IP를 리용한 NetBIOS를 사용할 때 콤퓨터열람기는 망상의 체계이름목록을 창조하고 유지한다. 또한 망이웃과 같이 체계우에서 동작하는 응용프로그람목록도 제공한다. 콤퓨터열람기의 특징은 다른 령역의 이름들이 체계에 의하여 검사되도록 령역을 추가할수 있다는것이다.

DHCP중계국

DHCP의뢰기와 봉사기가 서로 분리된 2개의 망토막에 있을 때 DHCP중계국은 두 체계사이의 중계기로서 동작한다.

DHCP중계국은 의뢰기의 DHCP요구가 DHCP봉사기가 있는 다른 망토막으로 전달되고 봉사기가 보낸 응답이 의뢰기로 전달되도록 중계기능을 실현한다. 우점은 매 론리적인 망마다 DHCP봉사기를 따로 설정하여야 하는 필연성을 제거한다는것이다. 중계국은

의뢰기와 같은 망토막에 또는 의뢰기와 DHCP봉사기의 망토막들사이 경계(경로기로서 동작한다.)에 위치할수 있다.

DHCP중계국은 IP규약설치를 요구한다. DHCP봉사를 지적하기 위한 IP주소가 적어도 하나는 필요하다.

Microsoft의 DHCP봉사기

DHCP봉사기는 NT봉사기가 IP주소정보를 자동적으로 망의뢰기들에 제공할수 있게 한다. 의뢰기가 DHCP요구를 내보내면 DHCP봉사기에 의하여 IP망에서 통신하는데 필요한 모든 정보 즉 IP주소, 부분망마스크, 령역이름, DNS봉사기 등이 응답으로 주어 진다.

DHCP봉사기는 IP규약설치를 요구한다. DHCP봉사기가 설치될 때 DHCP관리자를 위한 차림표가 관리도구차림표에 자동적으로 추가된다.

Microsoft의 DNS봉사기

Microsoft의 DNS봉사기는 NT봉사기가 의뢰기와 다른 DNS봉사기의 요구에 응답할수 있게 한다. DNS봉사기가 WINS변환을 리용하도록 구성되여 있다면 호스트이름정보는 NetBIOS이름체계에 기초한 WINS에 의하여 제공된다.

DNS봉사기는 대체로 본문파일형태로 수동적으로 유지되는 호스트이름정보를 요구한다. 만일 어떤 봉사기의 IP주소가 변경되면 그것을 반영하여 DNS표도 갱신되여야 한다. DHCP는 IP주소정보를 제공하는데 리용한다. 그러나 DNS는 어느 호스트이름에 어떤 IP주소가 배정되겠는가 하는데 대해서는 미리 알수 없다.

WINS변환을 리용함으로써 DNS봉사기는 WINS봉사기에 호스트정보를 문의할수 있다. DNS봉사기가 먼저 문의를 WINS로 통과시킨다. WINS봉사기는 IP주소와 호스트이름을 대응시킨 NetBIOS표를 리용하여 응답을 만들어 DNS봉사기로 보낸다. DNS봉사기에 의하여 응답이 의뢰기로 전송된다. DNS봉사기는 모든 의뢰기요구를 단독으로 처리할수 있다. 그러므로 두개의 봉사를 같은 NT봉사기에 설치할 필요는 없다.

DNS봉사기는 IP규약설치를 요구한다. DNS봉사기가 설치될 때 DNS관리자를 위한 차림표가 관리자도구차림표로 자동적으로 추가된다.

Microsoft의 인터네트정보봉사기

Microsoft의 인터네트정보봉사기는 NT봉사기에 Web, FTP, Gopher 기능을 추가한다. 설치하면 의뢰기들은 HTML페지에 접근할수 있고 FTP를 통하여 파일을 전송할수 있으며 파일들에 대한 Gopher탐색을 수행할수 있다.

Service Pack3에서는 IIS3.0, NT4.0에서는 IIS4.0, Windows 2000에서는 IIS5.0이 지원된다.

기정으로는 IIS설치에 의하여 Inetpub등록부가 창조되고 그 안에 4개의 등록부가 만

들어 진다. 첫 3개의 등록부들은 3개의 봉사기들을 위한 기본등록부들이다. 3개의 봉사를 위한 파일과 등록부들이 자기의 기본등록부아래에 놓이게 된다.

넷째 등록부는 스크립트를 위하여 사용된다. CGI와 WINCGI, Visual Basic, Perl 등으로 개발된 Web응용프로그람들이 이 등록부에 적재될수 있다. 또한 일부 표본스크립트들과 개발도구들도 포함된다.

주 의

> IIS와 관련된 취약성들이 몇가지 존재한다. 이것은 아마 NT조작체계자체의 경우보다 더 많을것이다. 그러므로 리용가능하고 안전한 모든 보안림시보수프로그람들을 설치하여야 한다. 또한 IIS등록부구조를 검열하고 적당한 허가준위를 설정하여야 한다.

IIS는 IP규약설치를 요구한다. IIS설치시에 Microsoft의 인터네트봉사기라는 차림표폴더가 봉사관리를 위하여 창조된다.

Microsoft의 TCP/IP인쇄

Microsoft의 TCP/IP인쇄는 NT봉사기가 렬인쇄데몬(lpd)이라는 UNIX인쇄를 지원할수 있게 한다. TCP/IP인쇄는 NT봉사기가 lpd를 지원하는 인쇄봉사기 또는 인쇄기가 직접 련결된 UNIX체계에서 인쇄할수 있게 한다.

IP인쇄는 또한 NT봉사기가 Microsoft의 의뢰기를 위한 인쇄교환기로 동작하도록 한다. NT봉사기는 IP규약을 거쳐서 lpd에 련결되며 이 자원을 NetBIOS우의 망자원으로 공유할수 있게 함으로써 NetBIOS만을 리용하는 Microsoft의뢰기들이 인쇄일감을 의뢰할수 있게 한다. NT봉사기는 인쇄일감을 lpd인쇄기로 보낸다.

Microsoft TCP/IP인쇄는 IP규약설치를 요구한다. 설치시에 LPR라는 새로운 인쇄기포구가 추가된다. 그림 14-21에 인쇄기포구창문을 보여 준다. LPR는 lpd인쇄기에 대한 원격접근을 제공하는 원격렬인쇄기(Line Printer Remote)이다.

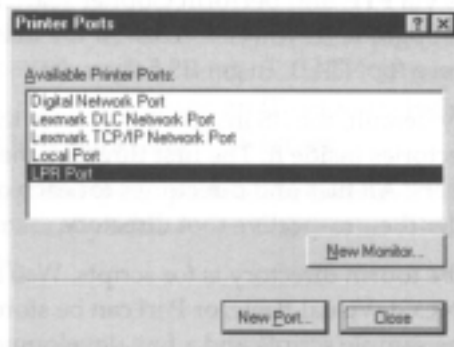



그림 14-21. IP인쇄설치시 LPR포구의 추가

망감시기관리자

망감시기관리자는 NT봉사기가 망감시기도구가 동작하고 있는 체계(NT봉사기)에 의하여 원격으로 감시될수 있게 한다.

망감시기도구와 관리자

망감시기도구는 NT봉사기로 들어 오고 나가는 모든 자료흐름과 방송프레임을 획득할수 있다는것을 제외하면 Novell의 LANAlyzer 또는 망일반탐지기와 류사한 망분석기를 설치한다.

그림 14-22. 망감시기도구에서 파케트획득

망감시도구는 봉사기가 분석목적을 위하여 망프레임을 획득하여 해득할수 있게 한다. 그림 14-22에서 망감시기도구의 파케트획득의 실례를 보여 준다. 도구는 원천과 목적주소, 리용한 규약들도 표시한다.

경 고

망감시기는 봉사기앞단에서 자료흐름을 감시할수 있는 아주 좋은 도구이다. 공격자들이 원격에서 망감시기자료에 접근할수는 있는데 보안실현을 위하여 중요하게 리용된다. 망감시기는 또한 유익하게 쓰이는 장애회복도구이다. 망감시를 하지 않는다면 반드시 무효로 되게 하여야 한다.

인터네트규약을 위한 RIP

인터네트규약봉사를 위한 RIP는 NT봉사기가 IP규약을 위하여 방송하는 경로정보를 리용하고 전파할수 있게 한다. RIP는 IP규약을 지원하는 동적경로조종규약으로서 NT설치시에 설정할수 있다. Microsoft의 Web싸이트에서 RRAS의 복사본을 내리적재할때에는 OSPF동적경로선택규약지원이 추가된다.

RPC구성

RPC구성봉사는 NT봉사기가 원격처리호출(RPC)를 지원할수 있게 한다. RPC는 국부체계에서 동작하는 응용프로그람이 원격체계에서 동작하는 응용프로그람이 제공하는 봉사를 요구할수 있게 한다. 응용프로그람이 정확히 수행되자면 두 체계가 RPC를 지원하여야 한다. RPC는 원격체계에 있는 부분프로그람의 호출을 지원한다는것을 제외하면 보통의 함수호출과 류사한 기능을 제공한다.

간단한 TCP/IP봉사

간단한 TCP/IP봉사는 Echo와 Chargen, Quote와 같이 자주 리용되지 않는 일부 IP응용프로그람들을 지원한다.

경 고

이러한 봉사가 필요하지 않으면 간단한 TCP/IP봉사는 설치하지 말아야 한다. 왜냐하면 DoS공격자들이 봉사기 또는 망전체에 대한 공격에서 Echo와 Chargen포구를 리용할수 있기때문이다.

Chargen포구는 문자를 수신하면 전체 자모수자표를 귀환하는것으로 응답한다. Echo포구는 자기에게 전송되는 모든 자료흐름을 검열하기 위하여 설계되였다. 두 체계가 이 두 포구사이에 통신하도록 지어는 단독봉사기가 그자체와 통신하도록 파케트를 위조하는 비법적인 DoS리용이 있다.

Echo포구는 Chargen포구로 매 문자를 보내고 Chargen포구는 다시 매 문자에 대하여 전체 자모수자표로 응답한다. 결과 망리용이 100%에 이르므로 목적지에 도착하여야 하는 합법적인 자료흐름이 차단된다.

SNMP봉사

SNMP봉사는 NT봉사기가 SNMP관리국에 의하여 감시되도록 한다. 또한 NT봉사기의 성능감시자가 IP통계자료와 IP응용(DNS, WINS 등)을 위한 통계자료를 감시할수 있게 한다.

SNMP봉사가 설치될 때 NT봉사기는 Hewlett-Packard의 HP Openview와 같은 SNMP관리국에 구성과 성능정보를 보낼수 있다. 이것은 NT봉사기와 SNMP장치의 상태가 집중

적으로 감시되게 한다. 감시는 IP 또는 IPX규약우에서 수행될수 있다.

SNMP봉사는 또한 NT성능감시기기능을 추가한다. 실례로 봉사기가 수신한 IP오유파케트의 수 또는 WINS문의의 수를 감시할수 있다. 또한 수신한 WINS요청의 수 또는 오유가 발생한 IP파케트의 수를 감시할수도 있다. SNMP봉사와 적용할수 있는 봉사는 둘다 성능감시기의 기능을 추가하기 위하여 설치된다.

Windows인터네트이름봉사(WINS)

WINS봉사기는 NetBIOS체계가 IP교갑화를 리용하여 경로기를 통하여 통신할수 있게 한다. WINS봉사기는 NT봉사기의 국부부분망에서 p마디점과 h마디점을 위한 NetBIOS이름봉사기로 동작한다. WINS는 체계의 NetBIOS이름뿐아니라 IP주소도 보관한다.

망상의 매 WINS봉사기는 자기의 NetBIOS표의 복사본을 가지고 있는 다른 WINS봉사기들을 주기적으로 갱신한다. 결과 망상의 매 체계에는 NetBIOS이름과 IP주소의 대응관계를 나타내는 하나의 동적인 목록이 존재하게 된다. 이 목록이 매 WINS봉사기들에 보관된다.

P마디점체계는 또 다른 NetBIOS체계의 주소가 필요할 때 자기의 WINS국부봉사기에 요청파케트를 보낸다. 요청이 원격부분망에 대한것이라면 WINS봉사기는 원격체계의 IP주소를 귀환한다. 이것은 원격체계가 망에 대한 방송프레임의 전파없이 IP주소를 알수 있게 한다. h마디점이 리용될 때에는 WINS봉사기가 특정호스트에 대한 입구점이 없다면 h마디점이 요청파케트를 방송한다는것을 제외하고는 기능상 p마디점과 같다.

WINS는 IP규약의 설치를 요구한다. 설치시 WINS관리자를 위한 차림표가 관리자도구차림표에 추가된다.

Windows NT에서 파케트려과

Windows NT는 IP자료흐름에 대하여 정적파케트려과기능을 제공한다. 려과기능이 좀 원시적이기는 하지만 보안기능을 추가로 제공하기 위하여 리용할수 있다. NT는 정적파케트려과기능을 리용할 때 상태유지는 불가능하다. 이것은 NT의 려과기가 합법적인 자료흐름과 공격자들에 의한 자료흐름을 구별할수 없다는것을 의미한다.

주 의

정적파케트려과와 동적파케트려과에 대하여서는 제5장에서 상세히 설명하였다.

Windows NT는 또한 파케트려과를 자료흐름의 어느 방향에 대하여 적용하는가를 지적할수 있다. 모든 려과는 경계내에로 들어 오는 자료흐름(SYN=1)에 대하여서만 진행된다. 이것은 NT의 파케트려과기능이 공격자가 체계에서 나오는 정보를 중계하는것은 막지 못한다는것을 의미한다. 결국 NT는 IP주소에 기초한 려과기능은 수행할수 없다. 이것은 접근조종방책이 모든 체계에 동일하게 적용된다는것을 의미한다. 다시 말하여 특정한 부분망으로부터의 접근만을 허용하도록 접근조종방책을 창조할수 없다.

파케트려과가능성

파케트려과를 허용하기 위하여서는 Network Properties → Protocols 에서 TCP/IP 규약을 두번 찰칵한다. TCP/IP 속성화면에서 IP 주소표적을 선택하고 창문의 오른쪽밑에 있는 상세(Advanced)단추를 찰칵한다. 그림 14-23 에 상세 IP 주소화면을 보여 준다.

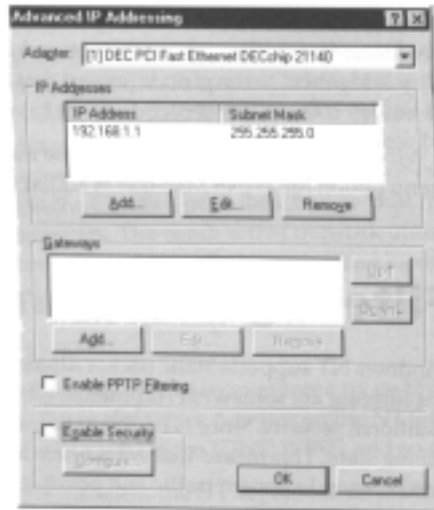



그림 14-23. 상세IP주소화면

여기서 보안허용검사칸을 유효로 한다. 다음 구성단추를 찰칵하면 그림 14-24에 보여 준 TCP/IP보안화면이 나타난다. TCP/IP보안화면에서는 파케트려과를 실현하는 접근조종방책을 구성할수 있다.

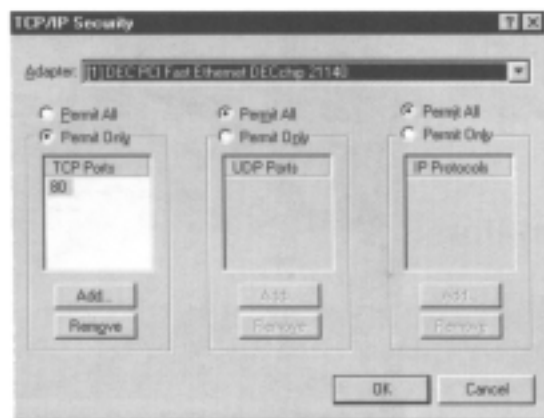



그림 14-24. TCP/IP보안화면

파케트려과구성

TCP/IP보안화면의 제일 우에는 망기판을 선택하는 차림표가 있다. 여기에는 체계에 설치된 모든 망기판들이 목록화되여 있다. 그러므로 모든 망기판들에 대하여 개별적으로 각이한 접근조종방책을 할당할수 있다. 두개의 부분망에 련결된 봉사기에서 각이한 봉사를 제공하도록 하는데 리용할수 있다. 실례로 봉사가 HTTP(TCP포구80)접근만이 가능하도록 제한할수 있다.

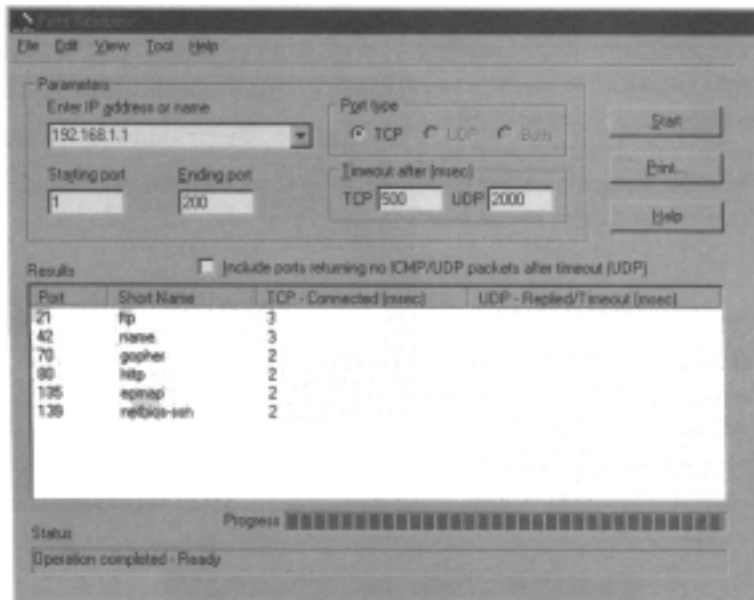



그림 14-25. 보호되지 않은 NT봉사기의 포구조사결과

TCP/IP보안화면에서는 어느 봉사가 선택된 망기판을 통하여 접근될수 있는가를 정의할수 있다. 실례로 그림 14-24에서는 DEC PCI망기판에 련결되지 않은 모든 사용자들에게만 TCP포구80인 봉사에 접근할수 있게 허용하고 있다. 이러한 접근규칙은 DEC PCI망기판에 직접 련결된 부분망뿐아니라 이 부분망의 뒤에 위치하는 다른 부분망에 대해서도 적용된다.

파케트려파설정의 효과를 리해하기 위하여 그림 14-25를 제시한다. 그림은 NT봉사기가 수행한 IP포구조사의 결과이다. 이 봉사기의 열린 포구들만을 검사하였다.

그림 14-26은 그림 14-24에 보여 준 접근조종방책을 구성한 다음의 같은 NT봉사기에 대한 포구조사의 결과이다.

봉사요구에 응답한 포구는 오직 TCP포구80(HTTP)뿐이다. 체계가 여러개의 부분망에 련결되여 있는 경우 파케트려파기능을 리용하여 Web봉사에 대한 접근만이 가능하도록 접근조종방책을 구성할수 있다.

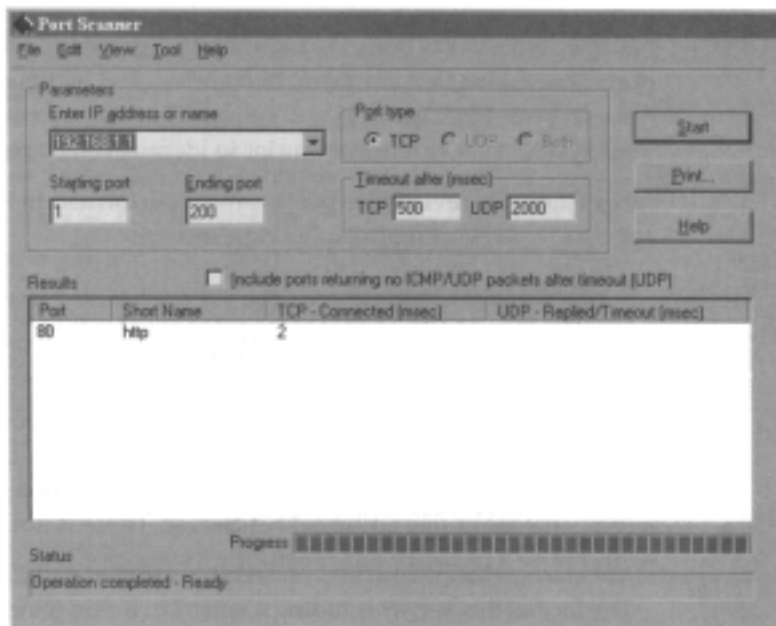



그림 14−26. 파케트려과를 리용한 NT봉사기의 포구조사결과

그림 14−24의 TCP/IP보안화면에는 IP자료흐름을 조종하는 3가지 선택창문들이 있다. TCP포구선택창문에서는 체계에 허용하는 내부로의 포구를 지정한다. 모두 허가선택단추를 유효로 하여 모든 TCP자료흐름을 허용할수 있다. 또는 유일허가선택단추를 유효로 하여 지정된 포구들에 대한 TCP자료흐름만을 허용하게 할수 있다. 새로운 포구의 추가는 TCP자료흐름만을 허용하게 할수 있다. 새로운 포구의 추가는 추가단추를 찰각하고 내부에로의 포구번호를 입력하면 된다. 이러한 려과설정은 SYN=로 설정된 TCP파케트에 대해서만 영향을 미친다. SYN기발이 설정되지 않은 자료흐름에 대하여서는 파케트려과기능이 무효하다.

주 의

NT파케트려과기능이 내부로 들어 오는 방향에 대해서만 유효하다는것을 명심하여야 한다. 이것은 응답을 요청한 호스트로 귀환시키기 위하여 포구번호를 열어 놓을 필요가 없다는것을 의미한다.

TCP자료흐름의 려과와 같이 NT의 파케트려과기능은 UDP자료흐름을 려과할수 있다. NT파케트려과가 동적이 아니라 정적이라는것을 명심하여야 한다.

이것은 NT가 UDP자료흐름의 려과에서는 실제의 방화벽만큼 효과적이 못된다는것을 의미한다. TCP자료흐름에 대하여서는 SYN기발의 설정에 따라서 려과가 결정된다. UDP는 기발을 리용하지 않으므로 선택할수 없다. 따라서 TCP/IP보안은 전송층준위의 접속형 자료흐름에 대한 려과기능을 제공하는데 리용할수 있다. IP규약선택창문에서는 추가단추를 찰각하고 특정한 전송층규약이름을 지정하여 려과기능을 수행하도록 할수 있다.

파케트려파기설정을 구성한 다음 반드시 OK단추를 찰칵하여야 한다. 또한 려파기능이 유효로 되자면 체계를 재기동시켜야 한다.

NT포구에 대하여 알아야 할 문제

NT는 둘이상의 응용프로그람이 어떤 특정포구에서 충돌한데 대하여 보고하지 않는다. 이것은 파케트려파에 의하여 차단된 포구가 사건보기로 오유통보문을 발생하지 않는다는것을 의미한다. 이것은 또한 어떤 봉사가 기동하고 있는지를 알기 위하여서는 체계를 매우 주의깊게 점검할 필요가 있다는 의미도 포함한다.

실례로 그림 14-25에서 보여 준 포구검열을 보자. 봉사기에는 다음의 봉사들이 기동하고 있다.

- WINS(Port 42)
- RPC(Port 135)
- NetBIOS over IP(Port 139)
- IIS

IIS는 포구21(FTP), 포구70(Gopher), 포구80(HTTP)을 리용한다. 이것은 보통의 NT봉사기와 같다. 이 포구들에 대해서는 망관리자의 의심을 자극하는 아무런 문제도 없다.

그러나 이 봉사에는 아주 큰 문제점이 있다. 만일 이 체계에서 telnet를 리용하여 포구70으로 원격접근하면 그림 14-27과 같은 지령대기화면이 나타난다. 통과암호가 요구되지 않으므로 즉시 파일체계에 접근할수 있다. 그러나 결과는 Gopher봉사기로부터 예견한 류형의 응답이 아니다.

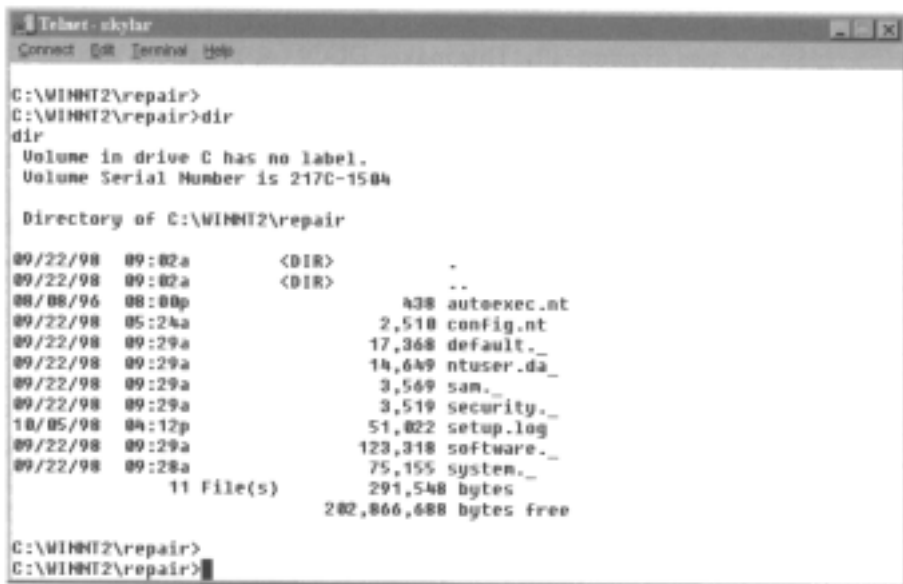



그림 14-27. 일반NT봉사기에서 나타나는 지령대화

어떻게 이런 일이 일어 났는가? NT봉사기에서는 NT용으로 제공되는 L0pht의 Netcat 복사판이 기동하고 있다. Netcat는 의뢰기뿐아니라 봉사기에서도 가동할수 있다. 또한 Netcat는 같은 포구번호로 대기하는 다른 봉사와 결합할수 있는 가능성도 가지고 있다. 따라서 Gopher봉사가 자료흐름을 검사하기전에 Netcate가 내부로의 봉사요구를 접수하여 처리할수 있다. 이것은 망관리자가 정확한 봉사가 대기하고 있는가를 확인하기 위하여 실지 매 능동포구에 대한 련결을 시도하여야 한다는것을 의미한다.

NT는 같은 대기포구에 결합하려고 시도하는 다중응용프로그람들사이 충돌은 보고하지 않기때문에 Netcat는 증거오유통보문을 생성하지 않는다. 심지어 Netcate를 기동하여 파케트려파방책에 의하여 차단되도록 가정한 포구에 대한 내부에로의 봉사요구를 대기하도록 하는것도 가능하다. 다시 말하여 요구가 려파되기전에 응용프로그람이 내부에로의 련결요구를 접수할수 있다. 또한 이런 류형의 동작은 오유기록통보문을 발생시키지 않는다.

일러두기

이 이야기의 교훈은 아무리 견고하게 체계를 차단하였다고 하여도 체계검열을 정상적으로 실시하여야 한다는것이다. 이 검열에는 주기억에서 어느 프로세스가 동작하고 있는가의 검사뿐만아니라 매 능동포구에 련결할 때 어떤 류형의 응답이 수신되는가의 검사까지 포함된다.

DCOM의 보안

분산요소대상모형(DCOM)은 원격처리호출(RPC)을 실현하는 대상지향방법이다. DCOM은 때때로 대상RPC라고도 한다. DCOM은 Microsoft의 대상련결과 매몰(OLE)기능을 원격으로 확장하기 위하여 설계되였다. OLE에 비한 DCOM의 우점은 조작체계의 다중특징을 지원하도록 설계된것이다.

DCOM의뢰기는 초기에 고정포구UDP135(NT RPC)로 DCOM봉사기와 련결한다. 그 다음 DCOM봉사기는 동적으로 포구를 할당한다. 이것은 DCOM응용프로그람이 NetMeeting과 Exchange와 같이 의뢰기자료흐름이 방화벽을 통과하여야 한다면 매우 복잡하게 된다는것을 의미한다. 단일 포구를 리용하는 대부분응용프로그람(실례로 TCP포구 25를 리용하는 SMTP)들과는 달리 DCOM은 1023이상의 모든 포구들이 열린 상태로 있을것을 요구한다. Windows플래트홈에 따라서 TCP포구들과 UDP포구들을 동시에 또는 각각 열어 놓을 필요가 있다. 이것은 명백히 DCOM응용프로그람이 방화벽을 넘어서 들어 오는 엄중한 보안위협을 받을수 있다는것을 의미하기도 한다.

DCOM전송의 선택

www.microsoft.com/com/wpaper/dcomfw.asp에 엠.넬손(M. Nelson)이 쓴 론문이 있다. 론문에서는 DCOM응용프로그람이 리용하는 포구범위를 어떻게 제한하는가에 대하여 설명하였다. 요약하면 Windows NT4.0을 제외하고 모든 Windows조작체계가 DCOM전송을 위하여 기정으로 TCP를 리용한다는것을 언급하였다.

일러두기

DCOM이 리용하는 포구번호를 제한하는 가장 좋은 한가지 방법은 모든 체계가 같은 전송규약을 리용하도록 하는것이다.

NT4.0체계에서 기정DCOM전송으로 TCP를 리용하도록 변경하기 위하여서는 regedt32를 기동하고 다음의 열쇠를 찾는다.

HKEY_LOCAL_MACHINE\Software\Microsoft\Rpc

그림 14-28. 등록고편집기를 리용한 DCOM의 기정규약변경

등록고편집기화면은 그림 14-28에 보여 주었다. 왼쪽 판은 특정열쇠를 찾기 위하여 검열할 필요가 있는 기본대상들을 보여 준다. 오른쪽 판은 실지 열쇠값을 보여 준다. 우의 열쇠는 DCOM이 리용하는 규약탐색순서를 정의한다. DCOM에 리용되는 첫번째 규약은 ncadg_ip_udp열쇠값에 의하여 정의된 UDP/IP이다.

이 열쇠를 지정하고 오른쪽 판에서 값을 두번 찰칵한다. 이때 그림 14-29에 보여 준 다중문자렬창문이 나타난다. 우에서부터 아래로 매렬은 DCOM이 리용하는 규약의 탐색순서를 정의한다. 실례로 그림 14-29에서는 DCOM이 UDP/IP를 리용하여 원격체계와 련결을 시도하고 련결이 실패하면 IPX를 리용하여 련결을 시도한다는것을 정의한다.

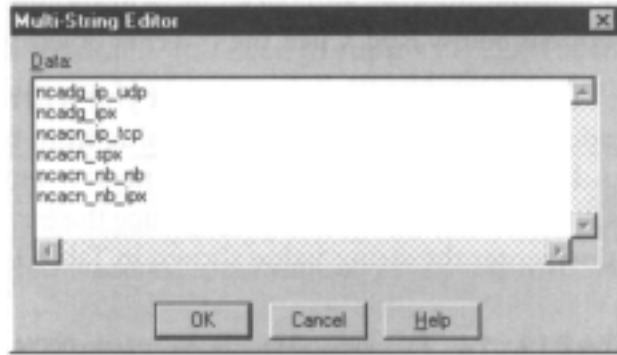



그림 14-29. DCOM의 규약탐색순서를 보여 주는 다중문자렬편집기

TCP/IP련결을 먼저 시도하도록 기정탐색순서를 변경하기 위하여서는 세번째 목록항에 있는 ncacn_ip_tcp를 Cut와 Paste를 리용하여 이동한다. 변경을 완성한 다음 OK단추를 눌러서 등록고편집기를 탈퇴한다. 변경이 유효로 되자면 체계를 재기동할 필요가 있다.

일러두기

다중문자렬편집기에는 Edit차림표선택이 없으므로 Cut에는 Ctrl+X를, Paste에는 Ctrl+V를 리용한다.

DCOM에서 리용되는 포구들의 제한

넬손의 론문에서는 또한 DCOM응용이 규정된 포구만을 리용하도록 포구범위를 어떻게 제한하는가에 대하여서도 설명하였다. 이것은 1023이상의 모든 포구들이 아니라 그 일부만을 제한함으로써 파케트려과기 또는 방화벽을 통하여 DCOM을 지원하는 부담을 덜어 준다.

주 의

이것은 어느 응용프로그람이 DCOM을 리용하는가는 제한하지 못한다. 즉 단순히 DCOM자체가 리용하는 포구들만을 제한한다.

DCOM이 리용하는 포구를 정의하기 위하여 regedt32를 기동하고 이 장의 마지막단락에서 편집한 열쇠로 돌아 간다.

HKEY_LOCAL_MACHINE\Software\Microsoft\RPC

열쇠를 지정하고 등록고편집기의 차림표에서 Edit→Add key를 선택한다. 그러면 Add key대화칸이 나타난다. 열쇠이름마당에 Internet를 입력하고 OK를 찰칵한다.

RPC아래에서 Internet라는 열쇠값을 볼수 있다. Internet대상을 찰칵하여 입구점을 지

정한다.

표 14-1에 이 열쇠에 추가할수 있는 값들을 보여 준다. 값들은 등록고편집기의 차림표에서 Edit→Add Value를 선택하여 추가할수 있다. Add Value창문이 나타나면 값이름과 자료형을 입구한다. OK단추를 찰칵하여 문자렬편집기를 연시한다. 문자렬편집기창문에서 표 14-1에 제시한 문자렬값을 입구한다.

표 14-1 DCOM이 고정된 포구번호들을 리용하도록 변경할 때 요구되는 열쇠

값 이 름	자 료 형	문자렬값
Ports	REG_MULTI_SZ	57100-571200
57131		
PortsInternetAvailable	REG_SZ	Y
UserInternetPorts	REG_SZ	Y

포구문자렬값은 DCOM의 어느 포구들을 리용하여야 하는가를 정의한다. 매렬은 특정포구번호 또는 포구범위를 지정한다. 실례로 표 14-1에서 포구57100-57120은 DCOM이 리용할수 있는 포구범위를 정의한것이다. 또한 추가로 57131이 정의된다. 방화벽을 거쳐서 DCOM을 지원하려고 한다면 포구열쇠와 결합되는 문자렬값들은 인터네트에서 봉사기로 열어 놓을 필요가 있는 내부에로의 포구번호들로 정의된다.

주 의

DCOM포구를 할당할 때 1∼49151포구들을 절대로 고정적으로 할당하지 말아야 한다. 그것은 이 포구들이 다른 봉사를 위하여 리용되든가 또는 DCOM응용이 기동하기전에 체계에 의하여 동적으로 할당되기때문이다. 정적인 포구배당시에는 49152∼65535사이의 포구번호들만 리용하여야 한다. 더 자세한 정보는 ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers 에서 참고하시오.

DCOM과 NAT

DCOM에 대한 한가지 경고는 렬 IP주소정보가 체계들사이를 통과한다는것이다. 이것은 망주소변환이 리용될수 없다는것을 의미한다. NAT는 사설적인 IP주소공간을 인터네트통신목적을 위하여 리용되는 합법적인 IP주소공간으로 변환하는데 리용된다. DCOM봉사기가 NAT기능을 수행하는 장치뒤에 있다면 DCOM은 동작할수 없다. 그것은 자료흐름에 NAT에 의한 IP주소변환을 요구하는 의뢰기통신도 포함되기때문이다. 만일 인터네트상에서 DCOM응용을 지원할 필요가 있다면 NAT를 IP주소정보를 변환하는데 리용할수 없다.

일러두기

만일 자료흐름이 VPN통로를 따라서 전송된다면 사설주소공간을 인터네트를 통하는 DCOM응용에 리용할수 있다. 이것은 통로가 NAT실행없이 사설주소공간을 리용하기때문이다. 더 자세한 정보에 대하여서는 제10장을 참고하시오.

Windows 봉사에 리용된 포구

Microsoft는 NT조작체계에 고유한 여러 포구들과 봉사들을 리용한다. SMTP, FTP, HTTP와 같은 봉사에 리용되는 포구번호들은 RFC 1700에 문서화되여 있지만 많은 포구번호들이 Windows의 고유한 봉사 즉 WINS와 원격사건보기 등을 위하여 리용되고 있으며 이러한 포구번호들은 RFC로 문서화되지 않는다. 이것은 Microsoft봉사를 방화벽 또는 파케트려과기가 리용되고 있는 부분망으로 확장하는것이 매우 어렵다는것을 의미한다.

표 14-2에 공통적인 Windows봉사들에서 리용하는 전송규약과 대응하는 포구번호들을 제시한다.

표 14-2 공통적인 Windows봉사들에서 리용하는 전송규약과 포구번호

이 름	전송규약/포구번호
b마디점찾기	UDP/137, UDP/138
p마디점 WINS등록	TCP/139
p마디점 WINS문의	TCP/139
WINS복제	TCP/42
가입	UDP/137, UDP/138, TCP/139
파일공유접근	TCP/139
인쇄기공유접근	TCP/139
사건보기	TCP/139
봉사기관리자	TCP/139
사용자관리자	TCP/139
성능감시기	TCP/139
Registry편집기	TCP/139

주 의

일부 경우에는 표 14-2에서 보여 준 포구번호들이상으로 열어 놓을 필요도 있다는것을 생각하여야 한다. 실례로 사건보기가 원격NT체계가 리용하는 IP주소를 알려고 한다고 하자. 국부LMHOSTS파일을 리용하지 않는다면 WINS가 리용하는 포구번호들을 열어 놓을 필요가 있다.

표 14-3에서는 DCOM을 전제로 하는 Windows응용들을 보여 준다. 봉사들은 하나 또는 여러 고정포구들을 리용할수도 있고 등록고변경이 문서화되지 않는 한 1023이상의 임의의 포구번호들도 리용할수 있다. 또한 RPC135는 TCP로 변경하지 않는 한 기정으로는 UDP이다.

표 14-3 DCOM을 전제로 하는 Windows응용

이 름	전송규약/포구번호
령역신뢰	UDP/135, UDP/137, UDP/138, TCP/139
DHCP관리자	UDP/135
WINS관리자	UDP/135
통보문대기렬	UDP/135, TCP &UDP/1801, TCP/2101, TCP/2103, TCP/2105
Exchange	UDP/135
Exchange	UDP/135

주 의

방화벽을 통한 의뢰기통신을 지원하기 위하여서는 Exchange봉사기에서 등록고열쇠들을 추가로 변경하여야 한다. 더 자세한 정보는 Microsoft의 지식문서 Q148732와 Q155831을 참고하기 바란다.

보충적인 등록고열쇠변경

Microsoft Web싸이트를 검열하면 보안강화를 위하여 수정될수 있는 여러개의 등록고열쇠들은 찾게 된다. 모든 열쇠입구점들은 regedt32도구프로그람을 리용하여 변경되여야 한다. 이전판인 regedit에서는 다중부분열쇠의 지원과 같은 regedt32의 일부 개선된 기능들은 지원하지 않는다.

주 의

이 장에서 이미 언급한바와 같이 등록고를 변경할 때에는 반드시 먼저 비상회복디스크를 만들어야 한다.

가입기발

어떤 등록고열쇠를 수정하여 Windows NT가입처리를 Ctrl+Alt+Del을 눌러서 가입기발이 나타나도록 변경할수 있다. 가입기발은 규정 또는 체계리용방책을 나타내는 대화칸이다. 사용자가 체계에 인증되기전에 OK단추를 찰칵 또는 Enter건누르기로 실제의 가입화면이 나타나도록 하여야 한다.

가입기발을 추가하기 위하여서는 regedt32를 기동하고 다음의 열쇠를 찾는다.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version \Winlogon

이 열쇠안에서 두개의 열쇠값Legalnotice Caption과 LegalNoticeText를 찾는다. 수정을 위하여 두개의 값들중 하나를 찰칵한다.

Legalnotice Caption값은 대화칸의 제목에 나타나는 본문이다.

LegalNoticeText값은 대화칸에 나타나는 실제본문이다. 변경한 다음 regedt32를 탈퇴하고 체계를 재기동하여야 한다.

마지막가입이름의 숨기기

편리상 Windows NT는 체계에 국부적으로 가입했던 마지막사용자이름을 보존한다. 이것은 다른 사람이 Ctrl+Alt+Del을 눌러서 체계에 인증되려고 시도할 때 그전의 가입이름을 리용할수 있는 가능성을 준다. 이러한 문제는 다른 사용자가 합법적인 가입이름으로 체계에 인증될수 있기때문에 고도의 보안이 요구되는 환경에서는 불합리하다.

Windows NT는 가입시에 마지막사용자이름이 나타나는것을 금지시키기 위하여 다음의 등록고열쇠를 제공한다.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon

등록고편집기차림표에서 Winlogon열쇠를 지정하고 Edit→Add Value를 선택한다.

값추가창문에서 REG_SZ자료형을 가진 DontDisplayLastUserName이라는 값이름을 추가한다. OK단추를 찰칵하면 문자렬편집창문이 나타난다. 여기서 문자렬값 1을 입력한다.

문자렬값을 입구한 다음 OK단추를 찰칵하고 regedt32도구프로그람을 탈퇴한다. 변경이 유효로 되자면 체계를 재기동하여야 한다.

Windows NT워크스테이션에서 등록고보안

망을 통하여 또는 국부기계로부터 Windows NT체계의 등록고를 편집할수 있다. Windows NT봉사기에 대하여서는 원격등록고접근은 관리자준위구좌로 제한된다. 그러나 Windows NT워크스테이션에 대하여서는 이러한 제한이 없다.

등록고접근을 NT워크스테이션에 대한 관리자로 제한하기 위하여서는 다음의 등록고열쇠를 찾는다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentcontrolSet\Control\ SecurePipeServes

먼저 이 대상밑에 Winregs라는 열쇠를 창조할 필요가 있다. 이를 위하여서는 등록고편집기차림표에서 SecurePipeServers를 지정하고 Edit→Add key를 선택한다.

열쇠를 창조한 다음 그것을 지정하고 Edit→Add Value를 선택한다. 값추가창문에서 REG_SZ자료형을 가진 REG_DWORD값이름을 추가한다. OK단추를 찰칵하면 문자렬편집

기창문이 나타난다. 문자렬값 1을 입력한 다음 OK단추를 찰칵하고 regedt32도구프로그람을 탈퇴한다. 변경이 유효로 되자면 워크스테이션을 재기동하여야 한다.

사건보기에 대한 접근보안

Windows NT는 기정으로 손님들과 형식적인 사용자(null users)들이 사건보기체계와 응용기록정보의 입구점들에 접근할수 있게 되여 있다. 이 정보는 체계의 취약성을 알아내려는 공격자에 의해 리용될수 있다. 보안기록정보는 사용자관리자의 기록검열관리설정에 의하여 접근이 조종되므로 면제된다. 체계와 응용기록정보가 관리자준위의 구좌에 의하여서만 접근되도록 하자면 다음의 열쇠를 조작하여야 한다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eve
ntLog\Application
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eve
ntLog\System

응용열쇠를 지정하고 Edit→Add Value를 선택한다. 값추가창문에서 REG_DWORD자료형을 가진 값이름RestrictGuestAccess을 입력한다. OK단추를 찰칵하고 문자렬편집기창문에서 문자렬값 1을 입력한다. OK단추를 찰칵하고 체계열쇠를 지정한 다음 우의 단계를 반복한다.

페지파일의 제거

페지파일은 Windows NT가 가상기억으로 리용하는 하드디스크구역이다. Windows NT는 기억관리를 위하여 비활동적인 정보를 물리기억으로부터 페지파일로 이동함으로써 더 많은 물리기억이 활동적인 프로그람에 의하여 리용되도록 한다. Windows NT체계가 정지될 때 이 정보가 완전히 제거된다는 담보는 없다. 그러므로 체계를 다른 조작체계에 의하여 기동시킬수 있는 공격자가 이 파일에 보관된 정보를 읽을수 있게 된다.

페지파일의 내용이 정지시에 깨끗이 제거되도록 하기 위하여서는 다음의 열쇠조작이 필요하다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

기억관리열쇠를 지정하고 Edit→Add Value를 선택한다. 값추가창문에서 REG_DWORD자료형을 가진 값이름 ClearPageFileAtShutdown을 입력한다. OK단추를 찰칵하고 문자렬편집기창문에서 문자렬값 1을 입력한다. 문자렬값을 입구한 다음 OK단추를 찰칵하고 regedt32를 탈퇴한다.

주 의

체계는 페지파일을 지우기전에 2번의 재기동이 요구된다.

Windows 2000

Windows 2000은 새로운 보안특징들을 포함한다.

- 현재의 령역구조에 대한 일반적인 보안구조를 개선하기 위하여 설계된 능동등록부
- 파일체계암호화
- kerveros version 5
- 공개열쇠증서봉사
- IPSEC 지원
- 스마트카드지원

능동등록부

NT4.0이 일반적이고 확장불가능한 등록부봉사를 제공한다면 능동등록부는 매우 유연하고 계층적이며 확장가능한 등록부봉사를 제공한다.

능동등록부의 기능을 3가지 측면에서 고찰할수 있다.

보관 능동등록부는 망객체들에 대한 정보를 계층적으로 보관한다. 이 정보는 사용자, 응용, 봉사들이 리용할수 있다.

구조 모든 망객체와 봉사들은 능동등록부안에서 대상으로서 보관된다. 령역, 나무, 수림, 신뢰관계, 기관단위, 싸이트와 같은 구성개념들이 포함된다.

림주장 능동등록부는 표준등록부접근규약을 리용하며 다른 등록부봉사 또는 응용프로그람들과 통신할수 있다.

능동등록부의 다른 특징들은 다음과 같다.

DNS통합 모든 능동등록부봉사들은 DNS를 리용하여 모든 망봉사들에 요청하고 결합하며 련결된다.

확장성 능동등록부의 구조는 확장가능하다. 이것은 새로운 대상클라스와 이미 존재하는 클라스의 새로운 속성을 관리자 또는 응용에 의하여 능동등록부에 추가할수 있다는것을 의미한다.

대상지향방책 그룹방책이라고도 하는 이 설정들은 사용자들의 자원접근과 이 자원이 어떻게 리용될수 있는가를 결정한다.

척도화 능동등록부는 하나이상의 령역이름들을 리용하며 매 령역에는 또한 하나이상의 령역조종기가 있다. 다중령역들은 하나의 령역나무도 결합될수 있으며 다중령역나무들은 하나의 수림으로 결합될수 있다. 하나의 령역을 가진 망은 하나의 나무, 하나의 수림으로 된다.

다중관리자복제 모든 령역조종기들은 등록부변경이 다른 령역조종기에 의하여 진행되고 그 다음차례로 다른 령역조종기들이 갱신된다는 측면에서는 본질상 같은 권한을 가진다. 만일 하나의 령역조종기가 오유로 인하여 정지되면 다른 령역조종기들이 그 기능을 인계받는다.

집중화된 보안 능동등록부는 망에 대한 매 사용자접근을 보증한다. 또한 접근 조

종은 등록부의 매 대상에 대하여뿐아니라 그것의 매개 속성에 대해서도 정의될수 있다.

호상운영성 경량급등록부접근규약(LDAP)은 능동등록부가 응용 또는 다른 등록부 봉사들과 대상정보를 공유할수 있게 한다.

파일체계암호화

NT4.0에서 파일에 대한 사용자접근은 접근조종목록(ACL)에 의하여 조종된다. 그런데 콤퓨터체계의 물리적인 조종을 잃어 버렸다면 어떻게 되겠는가? 가령 휴대용콤퓨터를 도난 당했다면 어떤 일이 생기겠는가? 공격자는 ACL과 관계 없는 다른 조작체계로 휴대용콤퓨터를 기동할수 있으며 필요한 정보들을 읽을것이다.

이러한 문제를 극복하기 위하여 Microsoft는 Windows 2000에 파일체계암호화(EFS)를 통합시켰다. EFS는 Windows에서 CryptoAPI구조의 우점을 가지는 공개열쇠암호화에 기초한다. 매개 파일은 우연적으로 발생된 열쇠(파일암호열쇠라고 한다.)에 의하여 암호화된다. 파일암호화는 대칭암호화알고리듬을 리용하지만 앞으로의 개정판에서는 다른 방법을 리용할것이다.

EFS는 NT파일체계(NTFS)와 통합된다. 림시파일이 창조될 때 모든 파일이 NTFS볼륨에 있는 한 초기파일의 속성이 림시마당에 복사된다. 초기파일이 암호화되면 EFS는 파일창조시에 속성의 전달된 림시복사본들도 암호화한다. EFS는 Windows 2000핵에 존재하며 파일암호열쇠는 페지화에 의하여 하드디스크와 교체되지 않도록 페지화되지 않는 기억공간에 보관하고 리용한다.

EFS의 다른 특징들은 다음과 같다.

사용자호상작용 기정으로는 암호화를 위한 관리자의 그 어떤 조작도 필요 없다. 암호화와 복호화는 파일별로 또는 등록부별로 구체적으로 조종할수 있다.

자료회복 W2K는 체계가 하나이상의 회복열쇠를 가지도록 구성되였을 때에만 EFS를 허용한다. 자료회복은 기관에서 해고된 직원에 의하여 암호화된 자료가 회복될수 있다는것을 예견하여야 하는 상업적환경 또는 암호열쇠를 분실한 경우에 리용된다.

지령렬 암호화도구프로그람은 사용자가 지령렬로 파일과 등록부를 암호화하고 복호화할수 있게 한다.

Keberos Version 5

W2K이전에 Microsoft는 사용자인증을 위하여 NTLM규약에 기초하였다. W2K에서 시작하여 Microsoft는 MIT에 의하여 개발된 개방형공업표준규약 Kerberos를 통합하였다. 현재 5번째 개정판인 Kerberos는 NTLM상의 모든 우점들을 제공한 신중하고 견고한 규약이다.

봉사기에 더 효과적인 인증 NTLM에서 응용봉사기들은 매 의뢰기들을 인증하기 위하여 령역조종기에 련결하여야 한다. Kerberos에서는 봉사기들이 의뢰기가 가지고 있는 자격증서를 검열하여 의뢰기를 인증한다. 자격증서는 전체 대화기간에 재리용할수 있다.

호상인증 NTLM에서는 봉사기들이 의뢰기들의 신분을 확인할수는 있다. 그러나 의뢰기가 봉사기를 확인하거나 봉사기가 다른 봉사기를 확인할수는 없다. Keberos는 아무것도 가정하지 않는다. 즉 련결되여 있는 대방들은 서로 상대방이 주장하는것만을 알수 있다.

위임인증 Windows봉사는 의뢰기를 대신하여 자원에 접근할 때 의뢰기대리를 담당한다. 일부 분산응용들에서는 전단봉사가 반드시 의뢰기를 대신하도록 설계되여야 한다. Kerberos규약은 봉사가 련결되는 의뢰기들을 대신할수 있는 대리기능을 가진다. 그러나 NTLM에는 그러한 기능이 없다.

단순한 신뢰관계 Kerberos의 우점의 하나는 Windows 2000령역들에 대한 보안권한들사이 신뢰가 쌍방향이며 이동가능하다는것이다. 어떤 령역에 대한 보안권한에 의하여 발행된 증서는 나무안의 임의의 령역들에서 접수된다.

호상운영성 Microsoft는 인증에 Kerberos를 리용한 다른 망에서도 W2K가 허용되도록 한 IETF(Internet Engineering Task Force)에 의하여 규정된 Kerberos표준을 따른다.

공개열쇠증서봉사

W2K이전에 암호화는 분해형과 분리형으로 실행되였다. 인터네트성장과 보급에 따라 망체계의 호상운영과 자료대화에서 대방의 인증 그리고 자료대화의 암호화들은 자료처리를 위한 최소한의 표준으로 되였다.

공개열쇠암호화는 현대망들에서 아주 중요한 3가지 가능성을 제공한다.

비공개 전자우편, 음성, 긴급통보문을 포함한 모든 망통신을 암호화
인 증 대화의 전기간 대화와 관련한 모든 신분을 확인
부인방지 대화기간 대방들사이 진행된 모든 거래관련정보들을 등록

고전적인 암호화는 자료암호화와 복호화에서 리용되며 서로 공유하여야 하는 비밀열쇠에 기초한다.

비밀열쇠의 분실 또는 파괴는 암호화된 자료를 취약하게 만든다. 한편 공개열쇠체계는 두개의 열쇠를 가진다. 즉 서로 공유하는 공개열쇠와 서로 밀접히 련관되여 유지되는 비밀열쇠이다. 이 열쇠들은 공개열쇠에 의하여 암호화된 자료는 반드시 해당한 비밀열쇠에 의하여 해득된다는 의미에서 또는 그 반대의 의미에서 공개열쇠와 비밀열쇠는 서로 보충관계에 있다.

실례로 Bob가 Alice에게 어떤 사적인 자료를 보내려고 한다면 Bob는 Alice의 공개열쇠를 리용하여 암호화를 한 다음 Alice에게 보낸다. 암호화된 자료를 받은 Alice는 자기

의 비밀열쇠를 리용하여 해득한다. 여기서 중요한 개념은 Alice가 세계의 임의의 사람이 자료를 암호화할수 있도록 자기의 공개열쇠를 자유로 배포할수 있다는것이다. 물론 암호화된 자료는 Alice자신만이 해득할수 있다. 가령 Bob와 Chuck가 둘 다 Alice의 공개열쇠를 가지고 있고 Bob가 Alice로 보낸 암호화된 통보문을 Chuck가 가로챘다고 하자. Chuck는 그 통보문을 해득할수 없다. 오직 Alice의 비밀열쇠에 의하여서만 해득이 가능하며 그것을 가지고 있는 유일한 사람은 바로 Alice이다.

앞의 실례가 비공개라고 한다면 인증과 부인방지는 어떠한가? 이를 위하여 서명의 개념을 보자. 서명이 암호화를 위하여 리용되지만 목적은 자료원본을 증명하는것이다. 가령 Alice가 세계에 자기의 어떤 통보문의 저자이라는것을 알리려고 한다면 Alice는 통보문을 자기의 비밀열쇠를 리용하여 암호화하고 공개적으로 통보문을 배포한다. 이 통보문을 해득하는 한가지 방법은 Alice가 자유로 배포한 공개열쇠를 리용하는것이다. 따라서 통보문의 저자가 Alice임을 증명할수 있다.

암호화와 서명은 비공개, 인증, 부인방지를 위하여 함께 리용된다. 이 봉사들을 제공하는 기본구조는 공개열쇠하부구조(PKI)로 알려 져 있다. PKI는 공개열쇠의 관리와 실행을 쉽게 하도록 하는 조작체계와 봉사들을 의미한다. PKI는 다음의 기능들을 제공한다.

열쇠관리 PKI는 열쇠의 발행, 검열, 취소뿐아니라 열쇠에 첨부된 신뢰준위의 관리를 단순하게 한다.

열쇠출판 PKI는 사용자들이 공개열쇠를 배포하거나 회수, 또는 공개열쇠가 유효인가, 무효인가를 결정할수 있는 단순한 형식화를 제공한다.

열쇠리용 PKI는 제3자의 응용프로그람이 쉽게 어떤 봉사결합(암호화와 서명)을 선택하여 실행할수 있도록 서로 통합시키는 기능을 제공한다.

공개열쇠는 PKI가 리용하는(비밀열쇠는 항상 개별적으로 보관된다.) 대상이지만 그것은 보통 수자증서로 묶음화된다. 증서에는 공개열쇠와 열쇠소유자이름과 같은 상세한 식별정보표를 포함한다. 속성들과 공개열쇠사이의 결합은 증서가 그것을 발행한 개체에 의하여 수자적으로 서명되기때문에 존재한다. 즉 증서에 있는 발행자의 서명은 증서의 인증과 정확성을 보증한다.

문제는 처음으로 증서를 발행한 개체의 합법성을 결정하는것이다. 방도는 증서계층의 개념에 있다. 어떤 계층에서 매 발행자(증서권한이라고도 한다.)는 비밀열쇠를 가지고 발행한 매 증서에 서명한다. CA의 열쇠쌍중에서 하나는 공개하여 그자체를 증서에 묶음화한다. 다른 하나는 더 높은 준위의 CA에 의하여 발행된다. 이러한 과정은 가능한 많은 준위에 걸쳐 계속할수 있다. 그러나 마지막에는 최상위준위의 CA가 있어야 한다. 이러한 CA를 뿌리증서권한이라고 하는데 이것은 자기자체의 증서에 서명한다. 명백히 말단사용자는 뿌리증서가 합법적이라는데 대하여서는 그대로 신뢰하여야 한다. Thawte와 Verisign과 같이 잘 알려 진 산업용CA들은 100만명의 사용자들에게까지 증서를 발행한다. W2K는 자기자체의 PKI를 포함하는데 이것은 증서표를 발행하는데 리용되며 또한 증서들을 관리하고 리용하는 봉사들도 제공한다. W2K PKI의 기본요소들은 다음과 같다.

증서봉사 이 주요PKI봉사는 기관이 자기자체의 CA로서 기관이 수자증서를 발행하고 관리할수 있는 가능성을 가질수 있게 한다.

능동등록부 등록부봉사로서 능동등록부는 PKI를 위한 출판봉사를 봉사한다.

PKI가능한 응용들 인터네트탐색기, Microsoft의 Money, 인터네트정보봉사기, Outlook, Outlook Express뿐만아니라 많은 제3자의 응용프로그람들이 W2K PKI를 리용할수 있다.

Exchange 열쇠관리봉사 Microsoft Exchange의 요소들은 전자우편을 암호화하고 서명하는데 리용되는 열쇠를 보존하고 회수한다.

Microsoft는 열린 PKI표준에 맞추기 위하여 노력하였다. 일부 표준들은 표 14-4에서 보여 준다.

표 14-4 W2K가 지원되는 PKI표준들

표 준	무엇을 하는가
X.509	수자증서의 형식과 내용을 조종한다.
CRL ver.2	증서취소목록의 형식과 내용을 조종한다.
PKCS계렬	공개열쇠교환과 배포를 위한 형식화와 동작을 조종한다.
SSL ver.3	Web대화를 위한 암호화를 제공한다.
SGC	수출복잡성없이 SSL과 같은 보안을 제공한다.
IPSec	IP를 리용한 망대화에 대하여 암호화를 제공한다.
PKINIT	최근에 만들어진 표준으로서 공개열쇠를 리용하여 Keberos를 사용하는 망에 가입한다.
PC/SC	스마트카드표준이다

IPSec

NT 4.0은 견고하면서도 규칙적인 망자료암호화를 제공하지 않음으로 하여 혼합망 그리고 대역정보전송이 요구되는 오늘의 환경에서는 치명적인 결점을 가지고 있다. W2K는 자료흐름이 2개의 기초준위에서 안전하다는것을 담보하는 IP보안규약(IPSec)을 포함한다.

수정 자료는 경로에 있어서 보호된다.

가로채기 자료는 경로에 있어서 보거나 복사될수 없다.

IPSec는 IP를 위하여 IETF가 설계한 열린 표준으로서 망준위의 인증과 자료무결성, 암호화를 지원한다. W2K가 지원하는 IPSec가 OSI모형의 전송준위아래에서 적용되므로 응용측면의 구성이 필요 없다. 이것은 또한 VPN을 아주 간단히 실현할수 있게 한다. W2K가 지원하는 추가적인 IPSec봉사는 다음의 기능들을 포함한다.

자료무결성 IP인증머리부는 통신과정에 자료무결성을 담보한다.

동적인 열쇠변경 하나의 대화주기동안에 임의의 시간간격으로 열쇠를 변경시키는 것은 공격으로부터의 체계보호를 훨씬 개선한다.

집중화된 관리 W2K관리자는 사용자, 작업그룹 또는 다른 규정에 기초하여 구체적인 보안을 정의할수 있게 보안방책과 려과기능을 설정할수 있다.

유연성 IPSec는 단일워크스테이션, 사용자, 그룹 또는 기업범위자료통신에 적용될 수 있다.

IPSec는 인증머리부(AH)와 교갑화된 보안자료(ESP)를 리용하여 비공개, 인증, 부인방지를 제공한다. AH는 원본인증과 무결성을 제공하고 ESP는 인증과 무결성에 따라서 비밀성을 제공한다. IPSec에서는 송신자와 수납자만이 보안열쇠를 알고 있다. 만일 인증자료가 유효이면 수신자는 자료가 의도한 송신자로부터 보내졌으며 변경되지 않았다는것을 알게 된다.

Microsoft는 IPSec의 실행에서 다음의 공업규격기술들을 포함하였다.

Diffie-Hellman 열쇠공유를 위한 최초의 방법인 Diffie-Hellman은 공개정보를 교환하는데 2개의 관계인자를 리용한다. 매 개체는 자기의 비밀정보에 따라서 다른 개체의 공개정보를 결합하여 서로 공유하는 어떤 비밀값을 발생한다.

하쉬통보문인증코드(HMAC) 자료무결성을 증명하기 위하여 리용되는 HMAC는 매 파케트에 대하여 수자증서를 만든다. 만일 파케트내용이 변경되면 모순되는 결과가 암호화된 수자증서로부터 계산되며 파케트는 페기된다.

자료암호화표준(DES) 비밀성을 강화하기 위하여 리용되는 DES는 암호블로크사슬(CDC)이라는 비밀열쇠알고리듬을 리용하여 자료암호화에 리용되는 비밀열쇠인 우연수를 만든다.

W2K의 IPSec를 지원하는 다른 보안규약들은 다음과 같다.

인터네트보안련합과 열쇠관리규약(ISAKMP) 이 규약들은 보안련합(SA)의 제정을 지원하는 기본구조를 정의한다. SA는 두 콤퓨터사이 보안통신을 위한 절차(열쇠와 같은)들을 정의하는 파라메터들의 모임이다.

무료접근열쇠결정 무료접근은 PFS(Perfect Forward Secrecy)를 리용하여 만일 열쇠 암호가 파괴되면 그 열쇠에 의하여 직접 암호화된 자료만이 손상될수 있다는것을 담보한다. 어떤 열쇠는 다른 추가열쇠를 계산하기 위하여 절대로 재리용할수 없으며 열쇠생성에 리용된 초기자료도 다른 열쇠계산에 절대로 리용할수 없다.

IPSec가 W2K안에 통합되여 있기때문에 능동등록부, 그룹방책, 증서봉사를 포함한 W2K의 PKI봉사우점들을 가질수 있다. 이것은 W2K에 강한 보안우점을 제공한다. 즉 보안봉사의 집중관리가 가능하다.

스마트카드

NT4.0의 사용자인증방법은 다른 제3자의 제품을 설치하지 않는 한 통과암호로 제한된다. 통과암호는 관리상 측면과 사용자측면(사용자에 의한 설정기능이 미약하며 다른 사람에 의하여 쉽게 추측될수 있다는것, 고급한 통과암호를 사용하자면 매우 불편하다는것 등)에서 수많은 문제들이 제기된다. 총체적으로 보안연구는 개체식별을 더 안전하면서도 쉽게 관리할수 있는 방법을 개발하는데로 나가고 있다. 비용과 기능사이 균형이 보장되면서 제일 대중화된 방법들중의 하나가 스마트카드이다.

스마트카드는 증서, 비밀열쇠, 기타 개인정보들이 기억된 집적회로를 리용하는 신용카드크기만 한 장치이다. 스마트카드는 스마트카드읽기장치를 가진 콤퓨터체계에 접근하는데 리용한다. 대체로 사용자는 자기의 스마트카드를 읽기장치에 대든지 또는 읽기장치로 통과시킨다. 그때 개인식별번호(PIN)와 같은 고유한 개인정보들이 입력된다. 이것은 ATM카드와 류사하다. 그러나 스마트카드에서는 자기테프우에 평문형태로 정보를 보관하지 않고 집적회로에 암호문형태로 보관한다.

스마트카드는 의뢰기인증, 가입, 안전한 전자우편과 같이 쏘프트웨어적으로만 해결할수 있는 보안기능을 강화하는데서 매우 효과적이다. 스마트카드는 다음의 특징으로 하여 여러 PKI쎈터들에 실지로 존재한다.

- 개인 정보와 함께 비밀열쇠를 보호하는 견고한 기억기를 제공한다.
- 개인정보와 함께 비밀열쇠를 보안연산들(인증, 수자서명, 열쇠교환)을 알 필요가 없는 체계의 다른 부분과 격리시킨다.
- 임의의 위치(직장, 가정, 도로상에서)에서 콤퓨터들사이 증서와 개인정보를 교환할수 있는 가능성을 제공한다.

전통적인 스마트카드는 비표준화로 해서 사용이 제한된다. 국제규격화기구(ISO)는 스마트카드개발을 규격화하기 위한 시도로서 ISO7816을 개발하였다. 1996년에 Europay,

MasterCard, VISA(EMV)가 ISO규격을 채용하면서 금융봉사업을 지원하도록 한가지 기능을 추가한 규정을 제정하였다.

유럽원격통신공업이 ISO7816에 대한 자기자체의 변경을 만들기 위하여 표준처리를 분리시킴으로써 대역이동통신체계(GSM)규정이 휴대용전화사용자들의 식별과 인증을 가능하게 하였다.

이 규정에는 콤퓨터공업의 요구에 맞는것이 하나도 없다. 그리하여 1997년에 PS/SC(개인콤퓨터/스마트카드)그룹(Microsoft를 포함하여 여러 주도적기업들로 형성되였다.)은 PC/SC규정을 내놓았다. 또한 이 규격들은 ISO7816에 기초하며 정보체계와 직접 관련된 문제들도 포함한다. Microsoft는 다음의 기술들을 리용하여 이 규격들을 실현한다.

CryptoAPI 이 요소는 스마트카드봉사제공자(SCSP)가 암호화를 모르고서도 W2K 안에 통합된 암호화특성의 우점을 리용할수 있게 한다.

Scard COM 비암호대면부인 Scard COM은 응용프로그람들이 일반스마트카드봉사에 접근할수 있게 한다.

W2K와의 통합으로 하여 스마트카드는 기관의 PKI에 대한 기본협력자로서 리용되며 동시에 높은 수준의 관리와 함께 위험을 방지할수 있게 한다.

요 약

이 장에서는 NT봉사기환경에서의 보안을 어떻게 실현하는가에 대하여 설명하였다. 또한 사용자구좌관리, 파일허가설정에 대하여서도 고찰하였다. 또한 보안림시보수프로그람설치의 중요성에 대해서도 설명하였다. 다음에 강력하고 집중적인 망보안관리하부구조를 제공하는 Windows 2000의 새로운 기술들에 대하여 고찰하였다.

다음장에서는 UNIX체계의 보안을 어떻게 실현하는가에 대하여 설명한다. 많은 환경들에서 여전히 특수용도의 응용프로그람을 위하여 UNIX를 사용하므로 UNIX조작체계는 많은 망환경들에서 전략상 중요한 요소로 되여 있다.

제１５장. ＵＮＩＸ

UNIX가 동작하는 체계의 안전을 위하여서는 조작체계의 동작을 완전히 파악하여야 한다. 대부분의 UNIX체계들은 GUI류형에 따르지만 일반적으로 Windows조작체계와 같이 기능들을 대충 적당히 파악하고 리용할수는 없다. 그렇다고 하여 수많은 기능들을 도움말을 일일이 조사하여 그것이 언제 리용되는가를 파악할수도 없다. UNIX에서는 일부 도구프로그람들이 X-Windows에서 조작하지만 지령렬로부터 거의 모든 조작을 할수 있게 되여 있다. 그러므로 조작체계에 정통하지 못한 사람들이 UNIX체계를 보안한다는것은 매우 힘들다.

UNIX를 배우게 되면 세계적으로 귀중한 자료대부분을 조종하는 공인된 체계들을 관리할수 있는 능력을 소유할수 있다. UNIX가 PC관련 등 일부 분야에서는 시장을 잃었지만 특수용도의 응용프로그람들을 지원하는데서는 여전히 주역을 담당하고 있다. UNIX는 또한 매우 안전한 응용봉사기를 지원하는 능력도 가지고 있다. 실례로 IIS가 동작하는 NT봉사기는 RPC(135)와 모든 NetBIOS포구(137-139)들이 열려 져 있을것을 요구하므로 취약성을 내포하게 되지만 Apache가 동작하는 UNIX체계는 봉사를 위하여 요구되는 포구(Web봉사에서는 포구80)들만을 열어 놓을것을 요구한다. 열린 포구수를 줄이는것은 공격자들이 체계에 대한 취약성탐색의 가능성을 줄일수 있게 하므로 체계의 보안성을 높일수 있게 한다.

UNIX력사

1969년에 벨연구소에서 개발한 UNIX는 현재까지 리용되는 가장 오랜 분산형망조작체계이다. UNIX는 톰프손(Ken Thompson)의 공로라고 말할수 있다. 그 당시 그는 벨연구소에서 대형콤퓨터에서의 다중정보계산체계(MULTICS)를 개발하고 있었다. 그런데 벨연구소는 어떤 원인으로 해서 이 프로젝트를 중지하고 공간려행(Space Travel)이라는 새로운 유희프로그람개발에 착수하였다.

그때 톰프손은 유희프로그람이 동작할수 있는 새로운 조작체계개발을 시작하였다. MULTICS아쎔블러코드가 DEC PDP-7을 위하여 다시 작성되였고 이 조작체계를 UNICS라고 이름 지었다.

유희프로그람 Space Travel의 범위를 넘어서 기능들이 보강되였으며 일부 상업적인 측면으로 확장할수 있는 UNICS조작체계에 드디여 벨연구소가 관심을 돌리기 시작하였다. 그후 1972년에는 UNIX라는 이름으로 첫 제품이 개발되였다. 그때의 설치기준은 10대였다. 1973년에 톰프손과 덴니 리츠히(Dennis Ritchie)는 조작체계의 이식가능성을 훨씬 더 높일수 있도록 핵심부를 C언어로 다시 작성하였다.

1974년에 IP규약이 개발되였고 UNIX조작체계에 통합되였다. 이때부터 여러개의 말단들이 하나의 단일한 UNIX체계에 접근할 필요가 더이상 존재하지 않았으며 이써네트라는 공유매체가 체계접근에 리용되였다. 이로서 UNIX조작체계는 비로소 실제의 망조작체계로 되였다.

1970년대 중엽에 벨연구소는 UNIX를 종합대학들에 공개하기 시작하였다. 그시기 UNIX를 벨전화회사가 여전히 조종하고 있었으므로 UNIX의 상업적판매에 의한 리득은 허용되지 않았다. 이런 리유로 하여 UNIX원천코드의 료금은 최소로 지불되였으며 결과 급속히 퍼지기 시작하였다.

UNIX가 종합대학들에 배포되면서부터 그 개발이 급속히 촉진되였다. 대학생들이 코드를 개량하고 새로운 기능들을 추가하기 시작하였다. 그중에서도 캘리포니아종합대학에서 UNIX를 개량하여 버클리 쏘프트웨어배포(BSD)로 배포하기 시작한것은 아주 주목할만한것이다. 여러가지 형태의 UNIX조작체계들이 출현하였으므로 벨연구소에 의하여 개발이 계속되고 있는 UNIX판본을 체계5(system V)라고 하였다.

UNIX조작체계는 기능이 풍부하고 다양한 플래트홈들을 지원하는것으로 하여 1980년대초에 많은 갱신판들이 급격히 출현하였다. AT&T는 그 시기 자기의 사용권방책으로부터 이러한 변화에 공헌하였다고 볼수 있다. AT&T는 UNIX를 발전시킴에 있어서 이름은 그대로 보존하여 다른 배포자가 UNIX갱신판을 자체로 이름을 달수 있게 하였다. 실례로서는 Solaris(Sun)와 HP−UX(Hewlett−Packard)를 들수 있다. Microsoft도 UNIX를 개정하여 XENIX로 발표하였다.

1987년에 AT&T는 싼마이크로시스템과 Microsoft와 함께 UNIX의 주요개정판들을 하나의 단일 배포판으로 결합시키는데 합의하였다. SVR4(System V Release 4)라는 이 갱신판은 XENIX, BSD, System V Release 3의 가장 좋은 특징들을 결합하였다. 이 갱신판이 1990년대에 UNIX의 사실상의 표준으로 되였다. 1993년에 6개의 다른 제작자들인 Hewlett−Packard, SCO(The Santa Cruz Operation), SunSoft, Univel, UNIX체계연구소들이 공동으로 COSE(Common Open SoftWare Environment)라는 규격을 만들었다. 같은 해에 AT&T는 UNIX를 Novell에 판매하였고 Novell이 1995년에 다시 그것을 SCO에 판매하였다. UNIX를 규격화하려는 노력이 여러번 반복되였음에도 불구하고 UNIX는 갱신에서 여전히《분산성》을 띠고 있다. 그러나 UNIX는 여전히 가치가 있는 조작체계이다.

FreeBSD

FreeBSD는 1990년대초에 Novell과 U.C.Berkeley를 복잡하게 했던 격렬한 법률상전쟁으로부터 출현하였다. 초기에 BSD의 i386갱신판을 위한 수정프로그람으로서 개발되였고 그 다음 Novell과 U.C.Berkeley사이의 소송이 해결된후 남아 있는 UNIX의 4.4BSD−Lite2갱신판을 약간 갱신하여 다시 만들어 졌다. FreeBSD은 조종가능한 개발모형을 리용함으로써 특별히 안전하면서도 자유로운 조작체계를 만들었다.

그러면 원천코드와 가격에 관하여 다같이 열린 모형을 채용한 FreeBSD와 Linux는 어떻게 차이나는가? 초기개발자에 대하여 본다면 FreeBSD는 리누스 토발즈(Linns Torvalds)에 의하여 조종되는 Linux와 같이 어떤 한 사람에게 의존하지 않는다. 그리고 FreeBSD는 UNIX의 이전 판본들과 BSD로부터 많은 기술들을 계승하였기때문에 비록 Linux가 급속히 갱신되고 있지만 FreeBSD의 망기능은 더 견고하고 성능도 높다. 다음으로 Linux가 UNIX의 다른 기본계렬인 SVR4로부터 갱신되였으므로 파일체계설계, 기동처리, 실행표준의 측면에서 서로 다르다.

다음문제는 사용권문제이다. Linux는 GNU CopyLeft사용권에 의존하지만(그것은 Linux개발에서 투자의 우점을 크게 제한한다.) FreeBSD는 더 많은 상업적투자를 허용하는 자체의 사용권을 가지고 있다.

끝으로 FreeBSD는 Linux(또는 심지어 UNIX의 주류갱신판)우에서 기동시킬수 있다. 한가지 부족점은 장치지원에서 Linux와 같이 포괄적이 못된다는것이다. 다시 말하여 비데오기판과 같은 일부 장치들을 지원하지 못한다. 그러나 FreeBSD는 최신 판본과 협조하여 쉽게 갱신하고 유지할수 있다. 일부 기관(Yahoo! 등)들은 차이점보다도 류사성이 훨씬 더 많다는 우점을 고려하여 두 체계를 동시에 설치하여 사용할것을 결정하고 있다.

Linux

Microsoft에 대항하여 Linux가 만들어 졌다는 이야기가 있다. 그러나 사실은 아주 단순하다. 옛말을 인용한다면 《불만족은 발명의 어머니이다.》라고들 한다.

1991년에 필란드 헬싱키종합대학 학생이였던 리누스 토발즈는 Intel 386처리기우에서 동작하는 조작체계를 선택하는 문제로 고심하고 있었다. DOS는 쓰고 싶지 않았고 UNIX는 구입하기 어려웠으므로 그는 Minix라는 그리 크지 않은 PC에 기초하여 자체의 UNIX모방기를 만들기로 결심하였다. 그때 리누스는 완전히 열린 개발형식을 취하여 OS 그자체가 발전해 나가야 한다고 생각하였다. 그리하여 인터네트상에 원천코드를 공개하고 방조자들에게 앞으로 자기의 OS개발을 도와 줄것을 부탁하였다.

이때 Linux가 즉시에 자기의 새로운 《OS생활》을 시작할수 있는 두가지 가능성이 있었다. 그것은 누구나 최신 판본과 이전 판본을 내리적재할수 있는 헬싱키종합대학의 FTP싸이트와 장치구동기, 콤파일러, 코드서고들을 추가하는 경험이 풍부한 많은 방조자들이였다.

Linux는 초기부터 누구나 다 상대적으로 완성된 조작체계(초기에는 완전한 특성표도 없이 하나로 되여 있음에도 불구하고)를 내리적재할수 있도록 완전히 결합된 환경에서 개발되였다.

시간이 지남에 따라 많은 방조자들의 노력에 의하여 Linux에는 망조작체계(NOS)가 성공하기 위하여 요구되는 다중과제, 기억관리 특히 망기능과 같은 모든 기능들이 추가되였다. 물론 토발즈에 의하여 핵심부의 중요변경사항이 조정되지만 쏘프트웨어에 대한 열린 방법은 상업적인 리익을 고려하는 쏘프트웨어분야(비록 Linux가 기술적으로 구입비용 또는 허가비용에서 자유라는 사실은 받아 들이지만)에서 일부 문제들을 발로시킨다. 그러나 이러한 문제들은 단순히 전통적인 조작체계들에서 상업적인 문제들을 조정하는 단일기관이 없기때문에 발생하는 문제들이다.

Linux가 UNIX와 같이 《분산성》으로 하여 손해를 보고 있음에도 불구하고 지난 몇년동안에 많은 회사들이 DNS, DHCP, HTTP와 같은 주위의 망봉사와는 다른 상업응용프로그람의 핵심부로 Linux를 경쟁적으로 채용하고 있다. 방대한 하드웨어와 플래트홈지원과 결합된 Linux는 현저한 상업적지원을 획득하였다. 실례로 IBM(IBM은 Compaq, Dell과 함께 자기의 주요봉사기제품들에 Linux를 미리 설치하여 제공한다.)과 Linux플래트홈에 자기의 제품을 탑재하려고 하는 주요응용프로그람제작자(Oracle, Informix를 포함)들은 Linux에 11억5000만딸라를 투자하였다.

UNIX파일체계

대부분의 UNIX조작체계는 파일이름이 254문자까지 허용하는 POSIX에 따른 파일체계이다. 이름달기규칙은 매우 구체화되여 있다. 그러므로 Myfile.txt와 myfile.txt는 서로 다른 파일로 된다. POSIX는 파일분할을 감소시키는 고성능파일체계이다.

UNIX는 디스크가 추가될 때 구동기문자대신에 설치점(mount points)을 리용한다. 설치점은 단순히 새로운 디스크의 보관고가 추가되는 등록부구조상의 한개 위치를 나타내는 점이다. 이것은 유연한 파일구조기능을 제공함으로써 정보를 쉽게 통합할수 있게 한다.

실례로 UNIX기계를 설치한 다음 2개의 물리적인 하드구동기를 리용한다고 하자. 일반적으로 첫 구동기는 조작체계를 위하여 전용으로 리용되고 두번째 구동기는 사용자를 위한 홈등록부로 리용된다.

OS를 C에 설치하고 사용자홈등록부를 D에 놓을 대신에 단순히 /home등록부밑에 모든 파일의 보관을 위한 두번째 구동기를 할당한다. 여기에는 홈등록부밑에 위치한 파일들을 제외하고 1차구동기에 있는 모든 파일들이 보관된다.

이러한 파일체계에는 몇가지 우점이 있다. 첫째로, 림시구동기의 추가가 투명하다는 것이다. 만일 위치를 알지 못하는 파일을 찾는다면 단순히 뿌리로 가서 단일한 하나의 탐색을 수행하면 된다. 매 추가구동기들에 대하여 탐색을 반복할 필요는 없다. 왜냐하면 모든 파일들이 등록부구조의 체계로 구성되여 있기때문이다.

설치점의 리용은 또한 갑자기 정지된 구동기로 인한 체계측 결함을 줄일수 있게 한다. 실례로 두번째 디스크가 잘못되였다면 전체 체계가 아니라 사용자홈등록부들만 잃어버린다. 이것은 두개의 디스크상에 전체 기록권구조를 련결한 NetWare와는 대조적이다. NetWare에서는 구동기들중 하나가 잘못되면 기록권우에 있는 모든 파일들은 모두 접근할수 없게 된다.

UID와 GID에 대한 리해

UNIX에서는 파일들이 자기의 사용자 또는 그룹과 정확히 결합되여 허가되도록 하기 위하여 두개의 번호를 리용한다. 사용자식별자(UID)는 가입등록이름을 식별하는 유일한 번호이다. 그룹식별자(GID)는 사용자가 소속되여 있는 그룹들을 유일하게 식별하는데 리용된다. UNIX체계에서는 파일이 체계에 보관될 때 사용자의 UID와 GID를 파일과 함께 보관한다. 가령 사용자의 UID가 501이라면 이 정보는 사용자가 창조한 모든 파일들에 등록되여 파일접근시에 소유자를 식별하는데 리용된다.

UID와 GID정보를 보관하기 위하여 두개의 파일이 리용된다.

password 매 사용자의 UID와 1차그룹의 GID를 식별한다.
group 매 그룹의 GID와 함께 사용자의 2차그룹의 GID를 식별한다.

이 장의 뒤부분에서 통과암호파일과 그룹파일을 상세히 설명한다. 여기서는 매 사용자는 UID에 의하여, 매 그룹은 GID에 의하여 식별된다는것만을 리해하자.

파일허가

UNIX에 하나의 주되는 보안부족점이 있다면 그것은 파일허가설정이다. UNIX에서는 3가지 클라스 즉 소유자, 그룹, 모든 사용자에 대하여 파일허가를 설정할수 있다. UNIX에서는 사용자가 파일에 접근할 때 또는 사용자가 속한 그룹에 있는 다른 사용자가 파일에 접근할 때, 체계의 그밖의 다른 사용자들이 파일에 접근할 때 허가를 서로 다르게 설정할수 있다. 허가설정은 읽기, 쓰기, 실행으로 제한된다. UNIX는 변경, 수정, 삭제와 같은 더 세부적인 허가설정들은 지원하지 않는다.

실례로 독자가 홈등록부에 serverpasswords.txt라는 파일을 가지고 있다고 하자(실제 이런 경우는 존재하지 않지만 설명을 위하여 가정한다.). 또한 독자가 admin이라는 그룹에 속했다고 하자. 독자는 자신이 이 파일에 읽기, 쓰기할수 있게, admin그룹의 성원들에 대하여서는 읽기접근만이 가능하게, 체계의 그밖의 사람들에 대하여서는 접근이 불가능하게 파일허가를 설정할수 있다.

이 설정에서는 몇가지 문제점들이 있다. 우선 첫째는 《그밖의 사람들》은 접근이 불가능하다고 하였지만 그들은 독자가 전체 등록부에 대한 읽기허가를 제거하지 않는 한 여전히 그 파일이 있다는것은 볼수 있게 된다. 그들이 serverpasswords.txt파일이 거기에 있다는것을 아는 이상 어떤 단계를 거쳐서 그 파일에 접근하려고 노력할것이다. 등록부에 대한 모든 접근제거가 일부 경우에는 접수할수 있지만 독자가 공유된 파일령역들과 작업하고 있는 그러한 환경에서는 불가능하다.

다른 문제는 허가가 너무 일반적이라는것이다. 실례로 admin그룹에 있는 Sean과 Deb 성원들에 대하여서는 이 파일에 대한 읽기와 쓰기접근을 허용하지만 admin그룹의 기타 다른 성원들에게는 읽기접근만을 허용하게 허가설정을 할수는 없다. UNIX는 복잡한 파일접근이 요구되지 않았던 시기에 나왔다. 그때에는 실지 몇년동안은 체계접근을 더 어렵게가 아니라 더 쉽게 하는데 기본을 두고 갱신이 진행되여 왔다.

주 의

뿌리라는 관리자구좌는 항상 모든 체계파일에 대한 완전한 접근을 가진다. 이러한 속성은 제거될수 없다.

파일허가보기

등록부파일목록은 ls(list)지령을 리용하여 볼수 있다. 이때 −l(long) 스위치를 리용하면 파일허가정보가 현시된다. −a(all)스위치를 리용하면 숨은 파일도 볼수 있다. ls지령의 출력실례는 다음과 같다.

```
[granite:~]$ ls −al
drwx−−−−−      3  cbrenton  user      512  Aug  25  18:15  .
drwxr−xr−x  5400  root      wheel   95744  Aug  28  17:01  ..
−rw−r−−r−−     1  cbrenton  user        0  Oct  31  1997   .addressbook
−rw−r−−r−−     1  cbrenton  user     1088  May   6  1997   .cshrc
−rw−r−−r−−     1  cbrenton  user      258  May   6  1997   .login
−rw−r−−r−−     1  cbrenton  user      176  May   6  1997   .mailrc
```

```
-rw-------   1  cbrenton  user   7881  Aug  25  18:15  .pine-debug1
-rw-------   1  cbrenton  user   8410  Aug  25  16:30  .pine-debug2
-rw-------   1  cbrenton  user   7942  Aug  25  15:08  .pine-debug3
-rw-------   1  cbrenton  user   8605  Aug  25  14:49  .pine-debug4
-rw-r--r--   1  cbrenton  user  11796  Aug  25  18:15  .pinerc
-rw-r--r--   1  cbrenton  user   1824  May   6  1997   .profile
-rw-r--r--   1  cbrenton  user     52  May   6  1997   .profile. locale
-rw-r--r--   1  cbrenton  user    749  May   6  1997   .shellrc
-rw-------   1  cbrenton  user   2035  Jul  13  14:33  dead. Letter
drwx------   2  cbrenton  user    512  Aug  25  16:29  mail
```

첫번째 행은 허가정보이다. 이 출력은 입구점의 류형과 입구점에 배당한 허가를 나타내는 10개 문자들로 이루어 진다. 횡선(-)으로 시작한 입구점은 규칙적인 파일이라는것을 나타낸다. 표 15-1에 유효한 첫번째 문자들과 그것에 따르는 입구점의 류형을 설명한다.

표 15-1 UNIX 파일류형

입구점의 첫 문자	설 명
-	파일
D	등록부입구점
L	원격등록부에 있는 파일에 대한 기호적련결
B	테프장치와 같은 주변장치접근에 리용되는 블로크장치
C	말단과 같은 주변장치접근에 리용되는 문자장치

나머지 9개문자는 3개문자씩 3개의 부분으로 나누어 진다. 첫 부분은 파일소유자에게 배당된 허가를 나타낸다. 우의 등록부목록실례에서는 모든 파일들이 사용자 cbrenton에 의하여 소유된다. 두번째 부분은 파일소유자그룹에 배당된 허가를 나타낸다. 우의 실례에서는 cbrenton은 그룹 user에 소속되여 있다. 그러므로 두번째 부분의 허가는 이 그룹에 적용된다. 마지막 세번째 부분은 체계에 대한 유효가입구좌를 가진 그밖의 모든 사용자들에게 배당되는 허가를 나타낸다. 표 15-2에 가능한 허가를 보여 준다.

표 15-2 UNIX 허가설정

입구점문자	설명
R	입구점은 읽기방식으로만 보거나 접근할수 있다.
W	입구점은 수정되거나 지워 질수 있다. 만일 등록부에 대한 배당이면 새로운 파일이 창조될수 있다.
x	입구점이 파일에 대해서라면 실행될수 있다. 등록부에 대하여서라면 탐색이 가능하다.

실례로 출력실례에서 파일 .login은 다음과 같이 해석된다.

- (−)이 파일은 규칙적인 파일이다.
- (r)파일소유자는 이 파일을 읽을수 있다.
- (w)파일소유자는 이 파일에 쓸수 있다.
- (x)파일소유자는 이 파일을 실행시킬수 없다.
- (r)소유자의 그룹은 이 파일을 읽을수 있다.
- (w)소유자의 그룹은 이 파일에 쓸수 없다.
- (x)소유자의 그룹은 이 파일에 쓸수 없다.
- (r)그밖의 모든 사람들이 이 파일을 읽을수 있다.
- (w)그밖의 모든 사람들이 이 파일에 쓸수 없다.
- (x)그밖의 모든 사람들이 이 파일을 실행시킬수 없다.

다음으로 등록부목록실례에서 등록부 mail에 대한 입구점을 보자. 소유자cbrenton은 이 등록부에 대한 읽기, 쓰기, 탐색허가를 가진다. 그룹 user를 포함하여 그밖의 모두는 이 등록부에 대한 아무런 허가도 가지지 못한다. 그러므로 이 등록부에 대한 접근을 시도하면 《허가금지》오유가 귀환된다.

파일허가변경

chmod도구프로그람은 파일 또는 등록부에 배당된 허가를 변경시키는데 리용된다. 각이한 형태들이 있지만 대부분 사용자들은 리용하기 제일 쉬운 수자체계를 많이 쓴다. 수자체계는 읽기, 쓰기, 실행허가에 옹근수값을 배당한다. 배당한 값들은 다음과 같다.

- r(read):4
- w(write):2
- x(execute):1
- No permissions:0

수값들을 조합하여 특정준위의 접근을 만들수 있다. 실례로 수값 6은 읽기, 쓰기허가를 나타낸다. 수값 5는 읽기와 실행허가를 나타낸다.

chmod를 리용할 때 허가는 3자리수자를 리용하여 설정한다. 첫번째 수자는 소유자의 허가준위를, 두번째 수자는 그룹의 허가준위를, 세번째 수자는 체계의 그밖의 사용자들에 대한 허가준위를 나타낸다. 실례로 지령

chmod 640 resume.txt

를 실행하면 다음의 허가준위가 설정된다.

- resume.txt소유자는 읽기, 쓰기접근이 가능(6)
- 소유자의 그룹은 읽기접근만이 가능(4)
- 그밖의 체계사용자들은 접근이 불가능(0)

다중사용자조작체계에서는 사용자들이 자기의 과제를 수행할수 있게 하면서도 가능한 접근허가를 제한하여야 한다. 대부분의 UNIX조작체계는 기정으로 아주 일반적인 허가준위를 설정하고 있으므로 사용자접근을 허용하기전에 파일체계를 조사하고 제한을 엄

격히 설정하여야 한다. 그런데 사용자들은 많은 체계파일들에 대하여 적어도 읽기접근만은 반드시 요구한다. 그러므로 사용자들이 체계를 조사하여 더 높은 접근준위를 가질수 있는 취약성이 드러날 가능성이 있다.

파일소유권과 그룹변경

접근조종을 유지하는 다른 2개의 도구프로그람으로서 chown과 chgrp가 있다. chown지령을 리용하여 파일의 소유권을 변경시킬수 있다. 이 지령은 파일과 등록부를 이동시키거나 창조할 때 리용할수 있다. 이 지령의 문법은 다음과 같다.

chown <switches> <new owner> <file or directory name>

제일 유용한 스위치는 소속관계를 등록부구조에서 재귀적으로 변경시킬수 있게 하는 −R스위치이다. 실례로 지령

chown −R lynn *

은 현재등록부뿐아니라 그 아래에 위치한 모든 부분등록부들에 있는 모든 파일들에 대한 소유권을 lynn사용자에게 준다. lynn사용자자체가 chown지령을 실행하여 이 파일들에 대한 소유권을 가질수는 없다. 반드시 뿌리사용자가 lynn사용자를 위하여 이 지령을 실행하여야 한다.

주 의

UNIX에서는 대소문자를 정확히 구별하므로 R는 반드시 대문자여야 한다.

Chgrp지령을 리용하여 그룹과 파일의 결합을 변경시킬수 있다. 이 지령은 파일을 1차그룹 또는 다른 그룹들과 결합할 때 리용한다. 실례로 passwd파일을 users라는 1차그룹과 결합하였다고 하자. 또한 독자가 users그룹과 admin그룹의 성원이라고 가정하자. 독자가 파일을 창조할 때 이 파일은 자동적으로 users그룹과 결합된다. 이것을 admin그룹과 결합되게 하려면 다음의 지령을 실행시킨다.

chgrp admin file−name

이 지령은 파일과 admin그룹의 결합을 변경한다. 현재 설정된 그룹허가는 users가 아니라 admin그룹과 결합되여 있다. chown지령과 같이 전체 등록부구조에서 모든 파일에 대한 그룹결합을 재귀적으로 변경하는데 −R스위치를 리용할수 있다.

구 좌 관 리

UNIX체계는 사용자와 그룹을 관리하는 측면에서 자립적이라고 볼수 있다. 이것은 다중UNIX체계에서 구좌정보를 매 체계단위로 나누어서 관리할수 있다는것을 의미한다. UNIX의 특징은 또한 NIS[이미 누런페지(Yellow Pages)라고 알려 져 있다.]의 갱신판인 망정보봉사+(NIS+)를 통하여 집중적으로 관리될수 있다.

NIS+는 다중체계에서 사용자와 그룹정보를 공유하도록 설계된 계층자료기지이다. NIS정보를 공유하는 체계의 집합을 령역이라고 한다. 령역에 대한 사용자접근을 주기 위

하여 관리자는 사용자의 구좌를 기본 NIS봉사기에 단순히 추가하면 된다. 만일 사용자가 령역안의 체계에 접근하려고 시도한다면 체계는 사용자가입을 확인하기 위하여 기본 NIS봉사기에 접촉한다. 이것은 사용자가 정의된 국부구좌가 없어도 체계에 대한 접근허가를 얻을수 있게 한다.

통과암호파일

모든 사용자인증요구는 passwd라는 통과암호파일에 기초하여 검증된다. 여기에 passwd파일의 실례를 보여 준다.

```
[cbrenton@thor /etc]$ cat passwd
root:Y2YeCL6KFw10E:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd:
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/var/spool/news:
ftp:*:14:50:FTP User:/home/ftp:
nobody:*:99:99:Nobody:/:
cbrenton:7aQNEpErvB/v.:500:100:Chris Brenton:/home/cbrenton:/bin/bash
deb:gH/BbcG8yxnDE:501:101:Deb Tuttle:/home/deb:/bin/bash
dtuttle:zVKShMTFQU4dc:502:102:Deb Tuttle(2):/home/dtuttle:/bin/csh
toby:PpSifL4sf5Mc:503:103:Toby Miller:/home/toby:/bin/bash
```

매행은 단일사용자를 위한 인증정보를 나타낸다. 입구점마당들은 두점(:)으로 구분된다. 왼쪽에서 오른쪽으로 매개 마당들의 의미는 다음과 같다.

- 가입이름
- 암호화된 통과암호
- 사용자식별자
- 1차그룹식별자
- 가입이름에 대한 설명(보통 사용자의 전체 이름)
- 사용자의 홈등록부위치
- 이 사용자를 위한 쉘 또는 지령렬해석기

뿌리사용자는 항상 UID와 GID가 0이다. 또한 FTP와 같은 처리들은 뿌리로 체계에서 기동하지 못하도록 유일한 UID와 GID를 배당한다. 그것은 공격자들이 이 봉사들중의 하나를 손상시킬수 있는 여러가지 위험을 제한하기 위해서이다.

별표(*)로 된 통과암호마당은 차단된 구좌를 나타낸다. 차단구좌를 리용하여 체계에 인증될수는 없다. 차단구좌는 사용자구좌를 무효화시키거나 동작중인 처리들을 보안하는데 리용될수 있다.

일러두기

쉘입구점이 공백 또는 구좌가 무효인 사용자는 체계에 telnet을 리용하여 원격으로 가입하거나 또는 조종탁으로부터 가입할수 없다. 이러한 기능은 POP와 IMAP와 같은 봉사들은 제공하지만 사용자들에게 telnet를 통하여 쉘접근하는것을 허용하지 않는 경우에 리용할수 있다.

통과암호마당

passwd파일출력실례에서 알수 있는바와 같이 파일에는 통과암호의 암호문이 보관되여 있다. 이것은 사용자의 체계인증에서 passwd파일의 정보가 필요하기때문이다. 이것이 또한 주되는 보안문제로 된다. 왜냐하면 체계에 대한 합법적인 접근을 가지고 있는 사용자에 의하여 passwd파일이 다른 콤퓨터로 복사될수도 있고 힘내기공격에 의하여 사용자 통과암호들이 해득될수도 있기때문이다.

UNIX는 사용자통과암호를 암호화할 때 매우 강한 암호화알고리듬을 리용한다. UNIX는 사용자통과암호를 암호열쇠로 한 56bit DES를 리용하여 모든 비트가 0인 평문을 암호화한다. 얻어 진 암호문은 사용자통과암호를 열쇠로 하여 다시 암호화된다. 이러한 처리가 총 25번 반복한다.

마지막암호문의 해득을 더 어렵게 하기 위하여 소금결정(grain of salt)이라는 두번째 열쇠가 리용된다. 이 《소금》은 그때의 정황에 따라 0과 4095사이 값을 가진다. 이것은 만약 두명의 사용자가 같은 통과암호를 가진다고 하여도 마지막암호문은 서로 다르다는 것을 보증한다. 실례로 passwd파일의 출력을 다시 보자. 사용자 Deb Tuttle은 2개의 구좌를 가진다. 그리고 같은 통과암호를 리용하지만 결과암호문들은 서로 다르다.

통과암호를 암호화하는데 리용한 《소금》값은 암호문의 첫 두개문자이다. Deb의 통과암호가 창조될 때 리용된 《소금》은 gH이고 dtuttle통과암호에 리용된 《소금》은 zV이다. 사용자가 체계에 인증될 때 《소금》은 암호문으로부터 추출되여 사용자가 입구한 통과암호를 암호화하는데 리용된다. 얻어 진 두개의 암호문들이 서로 같으면 사용자는 확인되고 체계접근이 허용된다.

UNIX 통과암호해득

UNIX는 암호화를 적용하여 passwd파일을 만들 때 일반적인 암호화를 리용한다고 말한다. 이것은 공격자가 25번 암호화된 파일자체를 직접 공격하는것이 아니라 암호화에서 열쇠로 리용된 실제의 통과암호를 찾으려고 하기때문이다. 그런데 암호문을 해득하자면 반드시 열쇠가 필요하며 이 열쇠가 바로 공격자가 해득하려고 하는 통과암호이다.

그렇다면 어떻게 UNIX통과암호를 해득하는가? 그것은 체계가 사용자를 인증하기 위

하여 하는것과 같은 처리를 적용하는것이다. 공격자는 통과암호를 알아 내려고 할 때 passwd파일의 암호문입구점에서 《소금》을 추출한다. 그 다음 여러 단어들을 규칙적으로 암호화하여 암호문과 일치되는 문자렬이 얻어 질 때까지 계속한다. 일치되는것을 찾으면 공격자는 정확한 통과암호를 알게 된다.

주 의

통과암호를 알아 내기 위하여 리용된 단어목록을 보관하고 있는 파일을 사전파일이라고 한다.

공격자는 암호문을 반대로 처리하여 통과암호를 알아 낼수는 없지만 힘내기공격을 리용하여 정확한 통과암호를 추측할수는 있다. 그러므로 공통적인 단어 또는 봉사기이름과 사용자이름과 류사한 단어들을 통과암호로 리용하지 않는것이 중요하다. 이러한 단어들이 보통 공격자가 시도하는 첫번째 단어들이다.

그림자통과암호

passwd파일의 통과암호문에 대한 사용자보기문제를 해결하는 한가지 방법은 암호문을 어딘가 다른 위치에 보관하는것이다. 이것이 그림자통과암호의 목적이다. 이것은 뿌리사용자만이 접근할수 있는 파일에 암호문을 보관할수 있게 한다. 또한 체계의 모든 사용자가 이 정보에 접근하는것을 차단한다.

그림자통과암호가 리용될 때 passwd파일의 통과암호마당에는 오직 문자 x만이 포함된다. 통과암호의 암호문은 shadow라는 파일에서 찾아야 한다. shadow파일의 형식은 모든 마당들이 두점(:)으로 구분되는 passwd파일과 같다. shadow파일의 매 입구점은 최소한 사용자가입이름과 통과암호를 포함한다. 또한 사용자가 자기의 통과암호변경이 허용되기전까지의 가능한 최소, 최대시간과 같은 통과암호수명정보도 선택적으로 포함할수 있다.

경 고

그림자통과암호를 리용하려면 먼저 리용하고 있는 다른 인증체계들이 shadow형식과 호환성이 담보되는가를 확인하여야 한다. 실례로 NIS(NIS+ 는 아니다.)의 대다수 이전 판본들은 통과암호정보가 passwd파일에 보관되여 있을것을 요구한다. 만일 이러한 체계들중의 하나에 그림자통과암호를 설치하면 NIS는 정지되며 체계에 더이상 접근할수 없게 된다.

그룹파일

이 장에서 이미 설명한바와 같이 그룹파일은 매 그룹 또는 그룹성원들과 결합되여 있는 GID를 식별하는데 리용된다. 대부분 UNIX판들은 사용자가 한개이상의 그룹에 소속되는것을 허용한다. 그룹파일의 실례를 아래에 보여 준다.

```
disk::6::root
lp::7:daemon, lp
mem::8:
kmem::9:
wheel::10:cbrenton
mail::12:mail
news::13:news
ftp::50:
nobody::99:
users::100:cgrenton, deb, dtuttle, toby
cbrenton::500:cbrenton
deb::501:deb
dtuttle::502:dtuttle
toby::503:toby
```

사용자 cbrenton, deb, dtuttle, toby들은 자기들의 가입이름을 공유하고 있는 고유한 그룹의 성원들이면서 또한 users그룹의 성원들이다. Passwd파일을 좀 더 조사하면 매 사용자들이 자기의 1차그룹으로서 가입이름과 같은 그룹을 가지고 있다는것을 알수 있다. 이것은 사용자들이 의도한 이상으로 접근이 배당되는것을 막을수 있으므로 보안기능을 강화할수 있게 한다.

사용자가 파일을 창조할 때 체계는 파일소유자뿐아니라 소유자그룹에도 읽기, 쓰기 접근을 제공한다. 이것은 사용자가 resume.txt라는 파일을 창조하였다면 사용자의 1차그룹에 속하는 모든 성원들이 그 파일에 대한 쓰기접근을 가지게 된다는것을 의미한다. 이것은 기정으로 일반적인 허가설정이 배당되여 있기때문이다. 즉 사용자가 chmod지령의 리용을 잘 모르거나 잊어 먹을수 있는 경우를 예상해서이다.

이러한 파일허가문제를 해결하기 위하여서는 매 사용자를 유일한 그룹으로 배당하여야 한다. 이것은 기정으로는 모든 다른 사용자들이 《그밖의 모두》에 의하여서 보여 지며 파일접근이 최소준위(보통 읽기)로 제공된다는것을 의미한다. 그러나 만일 다른 사용자를 더 높은 준위의 파일접근을 가지게 하려고 한다면 chgrp지령을 리용할수 있다. 이것은 더 높은 준위의 파일접근을 보증하기전에 무엇을 하여야 하는가를 먼저 고려해 보아야 한다는것을 의미한다.

실례로 사용자 cbrenton이 smtp.txt라는 파일을 창조한다고 하자. 파일목록은 다음과 같다.

```
[cbrenton @ thor cbrenton]$ ls -al smtp.txt
-rw-rw-r--    1 cbrenton  cbrenton        499  Feb  5  1997  smtp.txt
```

사용자 cbrenton은 cbrenton이라는 단일그룹에 있으므로 체계의 모든 다른 사용자들은 이 파일에 읽기접근만이 가능하다. Cbrenton이 deb, dtuttle, toby에게 쓰기접근을 허용하려

고 한다면 chgrp지령을 리용하여 이 파일과 users그룹을 결합하여야 한다. 지령의 문법은 다음과 같다.

chgrp users smtp.txt

이 지령을 실행한후에 smtp.txt의 목록은 다음과 같이 나타난다.

```
[cbrenton @ thor cbrenton]$ ls -al smtp.txt
-rw-rw-r--   1 cbrenton users        499 Feb 5 1997 smtp.txt
```

Users그룹의 모든 성원들(deb, dtuttle, toby)이 smpt.txt 파일에 대한 읽기, 쓰기접근을 가지게 된다. User그룹에 소속되지 않은 다른 모든 사용자들은 여전히 이 파일에 대하여 읽기접근만을 가지고 있다.

회전그룹(Wheel Group)

UNIX체계우에서 사용자는 su지령을 리용하여 또 다른 사용자의 신분으로 가정하는 것이 허용된다. su지령에서 가입이름을 밝히지 않으면 뿌리구좌로 가정하고 뿌리사용자 통과암호를 요구한다. su지령을 리용한 실례를 보여 준다.

```
[cbrenton@thor cbrenton]$ whoami
cbrenton
[cbrenton@thor cbrenton]$ su
password:
[root@thor cbrenton]# whoami
root
[root@thor cbrenton]# who am i
thor.foobar.com!cbrenton ttyp0 Aug 30 23:34(192.168.1.25)
[root@thor cbrenton]#
```

체계는 사용자의 현재 가입이름을 확인한다. Whoami지령의 출력에서 알수 있는바와 같이 체계는 사용자를 cbrenton으로 확인하였다. 그 다음 스위치없이 su를 입력하면 체계는 뿌리사용자의 통과암호를 요구한다. 통과암호를 입력하면 그이후의 whoami지령에서는 뿌리사용자로 확인한다. 그러나 Whoami지령을 리용하면 체계가 여전히 실제의 사용자를 알고 있다는데 대하여 생각하여야 한다.

이것은 누가 관리자권한을 람용하였는가를 추적할수 있는 아주 중요한 기능이다. /var/log/message파일의 마지막입구점을 검사하면 다음의 결과를 얻는다.

```
Aug 30 23:34:56 thor su: cbrenton on /dev/ttyp0
```

이 정보는 cbrenton이 언제 뿌리준위권한을 가정했는가를 나타낸다. 만일 비법적으로 뿌리권한을 람용한 사용자가 자기의 흔적을 없애기 위하여 이 입구점을 제거하려고 시도할것이 우려된다면 모든 기록입구점들을 원격체계로 보내도록 syslog를 리용할수 있다.

뿌리준위권한을 가정할수 있는 사용자들을 제한하는 한가지 방법은 그룹파일에서 회전그룹입구점을 리용하는것이다. 그것은 회전그룹의 성원들만이 뿌리준위권한을 가정할수 있기때문이다. 이 절에 있는 그룹파일을 조사하면 사용자 cbrenton만이 su지령을 뿌리권한으로 리용할수 있다는것을 알수 있다. 이것은 사용자 deb는 뿌리준위통과암호를 알고 있어도 자기의 구좌를 뿌리로 가정할수 없다는것을 의미한다.

사용자 deb는 뿌리사용자로 직접 체계에 가입하든가 먼저 구좌 cbrenton으로 들어갈 때만이 우의 기능이 가능하다. 이것은 뿌리준위구좌를 손상시키기 훨씬 더 어렵게 한다.

국부조종탁에로의 뿌리가입을 제한한다

앞에서 설명한바와 같이 deb가 뿌리준위통과암호를 알면 뿌리로 체계에 직접 가입하여 회전그룹보안을 우회할수 있다. 이것은 이 대화를 기록할수 있는 능력을 잃어 버릴수 있으므로 불리하다. 명백히 뿌리사용자가 체계에 만들수 있는 련결류형을 제한하는것이 유익하다.

실례로 뿌리구좌를 제한하여 가입이 오직 국부조종탁으로부터만 허가되도록 할수 있다. 이것은 뿌리사용자로 직접 가입하기 위하여서는 기계에 물리적으로 접근하여야 한다는것을 의미한다. 또한 이것은 체계에 원격으로(telnet와 같은 프로그람으로) 련결된 임의의 사용자가 첫 가입은 자기접근준위로, 그 다음은 su지령을 리용하여 뿌리준위로 접근할수 있다는것을 의미한다. 이것은 모든 원격사용자들에 대한 회전그룹제한을 실시할수 있게 한다.

대부분 UNIX체계들은 뿌리의 능력을 체계접근으로 제한한다. 대체로 /etc/securitty 파일에 입구점을 창조하여 진행한다. 실례로 securitty파일은 다음과 같다.

```
[root@thor /etc]# cat securetty
tty1
tty2
tty3
tty4
```

securetty파일안의 입구점들은 체계접근시 어느 대면부가 뿌리준위로 리용되는가를 식별한다. 체계의 직접말단대화는 tty로 식별된다. 이 파일은 뿌리가 첫 4개의 조종탁으로부터만 체계접근이 가능하다는것을 나타낸다. 그밖의 모든 다른 련결시도들은 거절된다. 이것은 deb가 telnet를 리용하여 뿌리준위로 체계에 접근하려고 한다면 비록 정확한 통과암호를 알고 있어도 거절된다는것을 의미한다. 이러한 대화의 실례는 다음과 같다.

```
Trying 192.168.1.200 (thor)...
Connected to thor.foobar.com
login: root
password:
Login incorrect
Login: root
Password:
Login incorrect
login:
```

실례에서 알수 있는바와 같이 체계는 telnet를 통하여 뿌리로 접근하는것을 허용하지 않는다. 공격자에 관해서는 뿌리통과암호가 변경될수 있다. 이것은 공격자가 다른 조종탁에서 체계에 접근하는것을 억제할수 있게 한다.

UNIX핵심부의 최적화

불필요한 봉사에 대한 핵심부지원을 제거하는것은 체계를 고정시키는 아주 좋은 방법이다. 이것은 체계성능을 최적화할수 있을뿐아니라 보안도 개선할수 있다. 실례로 UNIX체계를 경로기 또는 방화벽으로 리용한다면 파케트의 원천경로와 관련한 기능지원은 불필요하다. 이것은 공격자가 경로조종표를 우회하기 위하여 또는 속이기 위하여 원천경로조종을 리용하는것을 막을수 있게 한다.

UNIX핵심부의 구성은 매 실행에 따라 약간씩 변한다. 핵심부를 어떠한 구성으로 재구축할수 있는가는 제작자들이 어떤 선택들을 포함시켰는가에 관계된다. 설명을 위하여 Red Hat판 Linux와 작업한다고 하자. Red Hat는 UNIX핵심부를 재구축할 때 리용할수 있는 여러개의 도형화된 도구프로그람들을 지원한다. 일부는 어떤 플래트홈에서는 불가능하다.

주 의

Linux는 구성과 관련하여 대단히 많은 선택항목들을 지원한다. 만일 또 다른 UNIX에 대하여 핵심부를 재구축한다면 구성할수 있는 설정기능들은 제한된다.

Make의 동작

표준Linux핵심부는 최소의 공통요소들을 지원하도록 설계된다. 그러므로 Linux핵심부는 많은 체계들에서 동작할수는 있지만 특정한 구성으로 알맞게 최적화할수는 없다.

일러두기

대부분 배포판들은 ’386처리기를 지원하는 구성으로 핵심부를 설치한다. 고유한 하드웨어요구에 맞게 핵심부를 다시 콤파일하는것은 체계성능을 크게 최적화한다.

Red Had Linux에서 핵심부를 재구성하는데 리용되는 여러가지 지령들이 있다.

- make clean 혹은 make mrproper
- make config, make menuconfig 혹은 make xconfig
- make dep
- make zImage 혹은 make bzImage
- make modules
- make modules_install
- make zlilo 혹은 make bzlilo

매행의 지령들중에서 하나만을 리용하면 된다. Make clean지령은 꼭 필요하지는 않지만 실행시켜서 손해되는것은 없다. 모든 지령들은 /user/src/linux등록부에서 실행되여야 한다.

핵심부의 구성

항상 시작하기전에 핵심부의 상태를 보관하여야 한다. 이 방법은 무엇인가 비정상이 발생하면 항상 초기구성으로 돌아 올수 있게 한다. 핵심부의 파일은 /vmlinuz이다. 파일은 /vmlinuz.old로 복사하되 절대로 이동시키지는 말아야 한다. 핵심부의 구성과 관련한 파라메터들을 선택하는데는 세가지 지령들이 있다.

```
make config
make menuconfig
make xconfig
```

make config지령은 Linux에 정통한 관리자들에게 제일 익숙되고 제일 오래된 지령이다.

Make config대면부는 완전히 지령렬에 의하여 구동된다. Make config대면부는 아주 세부적인 설정기능을 기정으로 제공한다. 만일 지령재촉상태를 리해하지 못하면 그것을 변경할수 없다. 대답마당에서 질문표식을 설정하여 직결도움말에 접근할수 있다. 가장 큰 부족점은 가능한 기능들을 일일이 설정하여야 하는 복잡성이 있다는것이다. 차림표도구프로그람에서는 필요한 부분으로 이행하여 변경할수 있다. 그림 15−1에 make config가 수행될 때의 출력을 보여 준다.

Make menuconfig를 입력하면 그림 15−2에 보여 준 지령대면부가 나타난다. 화살표건을 리용하여 차림표선택들사이를 이동할수 있다. 지정한 선택에 대하여 y를 누르면 지원이 유효로, n을 누르면 무효로 된다. 일부 차림표항목에서는 모듈지원을 위하여 m을 선택할수 있다. 이것은 체계가 동작할 때 요구에 따라서 구동기를 적재 또는 제거할수 있게 한다. h를 누르면 기본도움말차림표로 돌아 간다.

```
[root@toby linux]# make config
rm -f include/asm
( cd include ; ln -sf asm-i386 asm)
/bin/sh scripts/Configure arch/i386/config.in
#
# Using defaults found in arch/i386/defconfig
#
*
* Code maturity level options
*
Prompt for development and/or incomplete code/drivers (CONFIG_EXPERIMENTAL) [N/y/?]
*
* Loadable module support
*
Enable loadable module support (CONFIG_MODULES) [Y/n/?]
Set version information on all symbols for modules (CONFIG_MODVERSIONS) [Y/n/?]
Kernel daemon support (e.g. autoload of modules) (CONFIG_KERNELD) [Y/n/?]
*
* General setup
*
Kernel math emulation (CONFIG_MATH_EMULATION) [Y/n/?]
Networking support (CONFIG_NET) [Y/n/?]
```

그림 15-1. make config의 출력

```
Linux Kernel v2.0.27 Configuration
------------------------------------------------------------------------------------
 +---------------------------------- Networking options ----------------------------------+
 |  Arrow keys navigate the menu.  <Enter> selects submenus --->.  Highlighted letters are  |
 |  hotkeys.  Pressing <Y> includes, <N> excludes, <M> modularizes features.  Press <Esc><Esc> |
 |  to exit, <?> for Help.  Legend: [*] built-in  [ ] excluded  <M> module  < > module capable |
 |                                                                                          |
 | +--------------------------------------------------------------------------------------+ |
 | |              [*] Network firewalls                                                   | |
 | |              [*] Network aliasing                                                    | |
 | |              [*] TCP/IP networking                                                   | |
 | |              [*] IP: forwarding/gatewaying                                           | |
 | |              [ ] IP: multicasting                                                    | |
 | |              [*] IP: firewalling                                                     | |
 | |              [ ] IP: firewall packet logging                                         | |
 | |              [*] IP: accounting                                                      | |
 | |              [ ] IP: optimize as router not host                                     | |
 | |              <M> IP: tunneling                                                       | |
 | |              <M> IP: aliasing support                                                | |
 | |              --- (it is safe to leave these untouched)                               | |
 | |              [ ] IP: PC/TCP compatibility mode                                       | |
 | |              <M> IP: Reverse ARP                                                     | |
 | +-----------v(+)-----------------------------------------------------------------------+ |
 Ã------------------------------------------------------------------------------------------
 |                        <Select>    < Exit >    < Help >                                  |
 +------------------------------------------------------------------------------------------+
```

그림 15-2. 차림표형핵심부구성화면

make xconfig지령은 X-Windows안에 있는 쉘로부터 기동하게 한다. make menuconfig와 류사하지만 더 편리하다. 또한 설정항목조사도 좀더 쉽다. 그림 15-3에 xconfig도구프로그램의 망부분화면을 보여 준다.

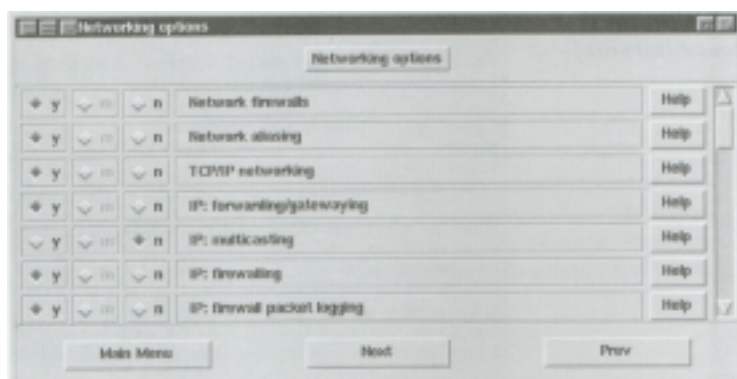



그림 15-3. X-Windows형핵심부구성화면

구성선택항목

선택방법에 관계없이 유효 또는 무효로 하는 특성들을 설정하는것이 중요하다. 망과 관련한 특성들의 요약된 설명을 아래에 목록화하여 제시하였다.

일러두기

더 완전한 목록은 직결도움말과 How-To파일에서 볼수 있다.

망지원? 망기능을 유효로 한다. 선택을 재촉할 때 Yes로 응답하지 않으면 다른 모든 망관련선택들을 조작할수 없다. 기정으로는 Yes이다.

주기억을 16MB로 제한? 이 설정은 16MB이상의 주기억관리시에 장애가 발생하는 이전체계들을 위하여 제공된다. 대부분의 체계들은 이 설정이 필요 없다. 기정으로는 no이다.

PCI BIOS지원? 이것은 하나이상의 PCI모선확장홈을 가진 체계지원을 제공한다. 대부분 새로운 체계들은 PCI를 지원한다. 기정으로는 Yes이다.

망방화벽? Linux체계가 방화벽으로 동작할수 있게 한다. 이 설정은 대체로 방화벽기능을 유효로 한다. 물론 IP의 방화벽기능만이 지원된다. 이 설정은 또한 IP로 통신하는것처럼 위장하려고 하는 경우 유효로 할 필요가 있다. 기정은 Yes이다.

망가명? 같은 대면부에 다중망주소를 배당할수 있게 한다. 현재 IP규약에서만이 지원된다. 같은 물리적인 토막에 두개의 론리적인 망을 구성할 필요가 있을 때 리용한다. 망기판을 여러개 사용하는 아파치Web봉사기를 리용하려고 계획한 경우 이 설정을 유효로 하여야 한다. 아파치는 각이한 IP주소들을 같은 망대면부에 배당하여 HTTP요구들을 같은 기계우에서 동작하고 있는 각이한 Web싸이트들에 보낼수 있다. 기정으로는 Yes이다.

TCP/IP망? IP망기능을 유효 또는 무효로 설정한다. IP를 리용하여 통신하려고 한다면 이 설정을 유효로 한다. 기정으로는 Yes이다.

IP:전달/교환기? Linux체계가 경로기로서 동작하여 IP자료흐름을 하나의 대면부로부터 다른 대면부로 전달할수 있게 한다. 국부망과 국부망 또는 국부망과

광지역망을 련결할 때 리용한다. IP로 통신하는것처럼 리용하려고 할 때 또는 체계가 방화벽일 때 이 설정을 유효로 하여야 한다. 기정으로는 Yes 이다.

IP:다중전송? IP다중전송을 리용할 때 또는 OSPF경로조종갱신정보를 전송하려고 할 때 이 설정을 유효로 하여야 한다. 기정으로는 no이다.

IP:방화벽? IP규약을 리용하여 방화벽을 지원할수 있게 한다. 이 선택은 또한 IP로 통신하는것처럼 위장하려고 할 때 또는 자료흐름을 구좌에 따라 관리하려고 할 때 그리고 투과적인 대리기를 리용하려고 할 때 유효로 설정하여야 한다. 기정으로는 Yes이다.

IP: 방화벽 파케트기록? 체계가 방화벽으로 리용될 때 이 설정은 통과하는 모든 자료흐름을 기록하는 파일을 창조한다. 또한 방화벽이 매 파케트를 접속 또는 거부하였는가를 등록한다. 기록은 누가 체계접근을 하고 있는가를 알아 내는 좋은 방법이다. 이 선택은 자주 리용된다. 그러한 정보가 필요 없다면 시간에 따라 등록정보를 단순히 지워 버리면 된다. 기정으로는 no이다.

IP:구좌관리? 체계가 방화벽 또는 망교환기로 동작할 때 이 선택은 통과하는 모든 자료흐름을 기록하게 한다. Linux가 내부망에서 경로조종을 한다면 기록정보가 대단히 커질수 있으므로 이 선택을 무효로 한다. Linux가 광지역망접속에서 경로조종 또는 방화벽기능을 수행하면서 경로조종을 할 때 광지역망리용정황을 위한 추적정보를 유지하려면 이 선택을 유효로 한다. 기정은 Yes이다.

IP:호스트가 아닌 경로기로 최적화? Linux가 정확히 경로기, 방화벽 또는 대리기로서 동작한다면 이 선택을 유효로 하여야 한다. 만일 체계가 HTTP, FTP, DNS 또는 다른 류형의 봉사를 제공한다면 이 선택을 무효로 하여야 한다. 기정으로는 no이다.

IP:통로화? 무선애호가 또는 이동IP를 위하여 리용할수 있는 IP파케트의 IP교갑화지원을 가능하게 한다. 기정으로는 필요할 때 체계가 적재한다는것을 의미하는 모듈지원이다.

IP 가명지원? 두개 또는 그이상의 IP주소를 같은 대면부에 배당할수 있게 한다. 망가명선택이 또한 유효로 설정되여 있어야 한다. 기정으로는 모듈지원이다.

IP:PC/TCP호환성방식? PC/TCP는 DOS형 IP규약탄창이다. 일부 호환성문제들이 있다. 즉 이전판본들은 같은 통신규칙에 완전히 따르지 않는다. 만일 PC/TCP가 동작하는 콤퓨터로부터 Linux체계에 련결할 때 장애가 있다면 이 선택을 유효로 한다. 그렇지 않은 경우에는 이 선택을 무효로 한다. 기정으로는 no이다.

IP:RARP? 이 선택은 대체로 디스크 없는 워크스테이션이 자기의 IP주소를 알아야 하는 경우에 리용된다. 선택을 유효로 하면 Linux체계는 이 요구에 응답한다. bootp봉사운영을 계획한다면 필요할 때 이 선택을 유효로 한다. Linux체계가 bootp 또는 DHCP봉사를 제공하지 않는다면 이 선택을 무효로 할수 있다. 기정은 모듈지원이다.

IP:MTU통로찾기무효? 최대전송단위(MTU)는 체계가 원격기계와 통신할 때 리용하는 가장 큰 파케트크기를 알아 낼수 있게 한다. MTU가 무효이면 체계는 현재 전송에서 항상 가장 작은 파케트크기를 리용하는것으로 가정한다. 이 선택이 통신속도에 크게 영향을 주므로 호환성문제를 고려하지 않을 때 MTU를 리용하여야 한다. 기정으로는 no로서 MTU를 유효로 한다.

IP:프레임의 원천경로조종중단? 원천경로조종은 전송국이 응답전송을 위하여 망경로를 지정할수 있게 한다. 이것은 요구에 응답하는 체계가 국부경로조종표에 따르는 경로대신에 지정된 경로에 따라 전송할것을 요구한다.

주 의

외부에 있는 잠재적인 공격자들은 공격하는 망내부에 있는것처럼 위장하기 위하여 원천경로조종프레임들을 리용할수 있다. 원천경로조종은 콤퓨터가 있다고 주장하는 망을 향해서가 아니라 다른 방향으로 프레임을 보내는데 리용된다. 인터네트가 제공하는 방향으로가 아니라 이런 목적에서 원천경로조종이 리용될 때 그것을 IP속임이라고 한다.

통표고리와 FDDI와 같은 망위상구조들은 규칙적인 통신을 위하여 원천경로조종을 리용한다. Linux가 통표방식의 위상구조들과 하나라도 련결되여 있으면 원천경로조종이 유효로 되여야 한다. 통신에 이러한 위상구조들이 리용되지 않으면 보안강화를 위하여 이 설정을 무효로 하여야 한다. 기정으로는 Yes이며 모든 프레임의 원천경로조종이 취소된다.

IP:큰 창문크기를 허용? 이 선택은 많은 프레임들을 응답없이 전송될수 있도록 전송완충기공간을 증가시킨다. 이것은 Linux가 매우 먼 거리(실례로 대륙사이 련결)에 있는 두 싸이트들을 련결하는 고속광지역망(다중T1 또는 그보다 더 고속인 망)에 직접 련결될 때 리용한다. 완충기공간의 추가는 주기억공간을 추가로 요구한다. 그러므로 이러한 규칙에 맞으며 적어도 16MB의 주기억을 가진 체계에서만 유효로 할수 있다. 기정은 Yes이다.

IPX규약? IPX규약지원을 가능하게 한다. 어떤 IPX봉사를 구성하려고 한다면 반드시 유효로 하여야 한다. 기정은 모듈구성이다.

완전한 내부IPX망? NetWare봉사기는 핵심부OS와 부분체계들사이 통신을 위하여 내부IPX망을 리용한다. 이 설정은 우의 개념을 한단계 더 확장하여 내부IPX망이 가상호스트를 지원할수 있는 정규망으로 확장시킬수 있게 한다. 이 설정은 단일Linux체계가 다중NetWare봉사기로 동작하는것처럼 보이도록 기존기능을 더 확장할수 있게 한다. 현재 기능의 《확장》이 필요 없다면 이 설정을 무효로 한다. 기정으로는 no이다.

AppleTalk DDP? 이 설정은 AppleTalk규약의 지원을 가능하게 한다. Netalk묶음(Linux가 AppleTalk를 위하여 지원한다.)이 리용될 때 Linux체계는 Mac의뢰기에 파일과 인쇄기봉사를 제공할수 있다. 기정으로는 모듈지원이다.

무선애호가 AX.25수준 2? 이 선택은 무선애호가통신을 지원하는데 리용된다. 이 통신은 점대점 또는 IP의 교갑화를 리용한 경우이다. 기정으로는 no이다.

핵심부/사용자 망련결구동기? 이 선택은 핵심부와 사용자처리사이의 통신을 지원하기 위하여 설계되였다. 2001년에 이 구동기는 여전히 시험적이며 제품화된 봉사기들에서는 요구되지 않는다. 기정으로는 no이다.

망장치지원? 이 설정은 망통신을 구동기준위에서 지원할수 있게 한다. 망기판지원은 광지역망통신을 위하여서는 유효로 하여야 한다. 기정으로는 Yes이다.

가상 망구동기지원? 이 설정은 순환귀환(loopback)주소의 리용을 허용한다. 대부분 IP체계는 IP주소 127.0.0.1로의 전송을 체계자체에로 다시 귀환시키는 자료흐름으로 인식한다. 이 선택은 일부 응용프로그람들이 순환귀환주소를 리용하여야 하기때문에 필요하다.

EQL(직렬회선 부하조정)지원? 이 선택은 Linux가 두개의 전화련결상에서 망부하를 조정할수 있게 한다. 실례로 가능한 대역을 중복시킴으로써 두개의 서로 분리된 선들을 통하여 인터네트봉사제공자를 호출할수 있다. 기정으로는 모듈지원이다.

PLIP(병렬 포구)지원? 이 선택은 가상인쇄기케블을 리용하여 두 체계사이 통신을 지원할수 있게 한다. 두 체계가 성공적인 통신을 보장하기 위하여서는 쌍방향병렬포구를 리용하여야 한다. 이것은 더 빠른 통신을 지원한다는것을 제외하면 가상모뎀케블을 리용하여 직렬포구로 두 체계를 련결하는 경우와 류사하다. 기정으로는 모듈지원이다.

PPP(점대점)지원? 이 선택은 Linux체계가 PPP광지역망련결을 창조 또는 접수할수 있게 한다. Linux체계가 전화가입련결을 창조하도록 리용하려고 한다면 유효로 하여야 한다. 기정으로는 모듈지원이다.

SLIP(직렬회선)지원? SLIP는 PPP의 이전 판본이다. 두 체계사이의 IP련결을 제공하며 전자우편전송에서 광범히 리용된다. PPP에 제공된 추가적인 특징들의 우점으로 하여 SLIP는 많이 쓰이지 않는다. 기정으로는 모듈지원이다.

무선통신망대면부? Linux체계가 확산스펙트르통신을 지원할수 있게 한다. 확산스펙트르는 무선국부망통신에서 거의 공통적으로 리용된다. 라지오대면부를 구성하기 위하여서는 이 설정을 유효로 하여야 한다. 기정으로는 no이다.

이써네트(10 또는 100Mbit)? Linux체계가 이써네트망기판을 리용하여 통신할수 있게 한다. 이써네트구동기를 선택하려면 유효로 하여야 한다. 기정으로는 Yes이다.

3COM기판? 이 선택은 3COM망기판목록에서 망기판을 선택할수 있게 한다. 무효로 하면 그 어떤 3COM망기판선택도 할수 없다. 유효로 하면 Linux가 지원하는 3COM기판의 선택이 가능하다. 기동시에 Linux는 매 망기판의 리용설정정보를 탐색하고 자동검사한다. 때때로 ISA카드에 대하여서는 틀리지만 정확도는 상당히 좋다. 체계는 재기동할 때 구성파라메터를 조사하고 망기판을 선택한다. 정확하면 모두 설정되고 틀리면 기판설정 또는 구성파라메터들을 변경하여야 한다. 망기판은 구성도구프로그람을 리용하여 설정된다. 기동설정은 Red Hat의 조종탁에서 핵심부데몬구성선택을 통하여 변경될수 있다. 기정은 Yes이다.

AMD LANCE와 PCnet(AT1500과 NE2100)? AMD와 PCnet망기판의 지원이라는것을 제외하면 3COM선택의 경우와 류사하다. 기정으로는 Yes이다.

Western Digital/SMC기판? Western Digital과 SMC망기판의 지원이라는것을 제외하면 3COM선택의 경우와 류사하다. 기정으로는 Yes이다.

다른 ISA기판? Cabletron의 E21계렬 또는 HT의 100VG PC국부망과 같은 일부 망기판들을 더 정확히 지정한다는것을 제외하면 3COM선택과 류사하다. 유효로 하면 Linux가 지원하는 여러 류형의 망기판을 선택적으로 지원할수 있다. 기정으로는 Yes이다.

NE2000/NE1000지원? 일반적인 이써네트망기판지원이다. 앞의 선택들에서 목록화되지 않은 망기판을 선택하려는 경우 유효로 설정한다. 기정으로는 모듈지원이다. 대부분의 이써네트망기판들은 NE2000과 호환성이 보장된다. 이 선택은 좀 포괄적인 의미를 가지고 있다.

EISA, VLB, PCI, 모판조종기우에서? 주기판에 직접 설치된 여러가지 망기판들도 있다. 유효로 하면 Linux가 지원하는 여러가지 류형의 망기판(주기판에 직접 설치되여 있다.)들을 선택할수 있다. 기정으로는 Yes이다.

휴대용적응기? Linux는 또한 병렬포구망 적응기를 지원한다. 유효로 하면 Linux가 지원하는 여러가지 병렬포구적응기들을 선택적으로 지원하게 할수 있다. 기정으로는 Yes이다.

통표고리구동기지원? Linux는 통표고리망적응기집합을 지원한다. 유효로 하면 Linux가 지원하는 여러가지 통표고리망적응기들을 선택적으로 지원하게 할수 있다. 기정으로는 Yes이다.

FDDI구동기지원? Linux는 몇개의 FDDI망적응기들도 지원한다. 유효로 하면 Linux가 지원하는 각이한 FDDI망기판들을 선택적으로 지원하게 할수 있다. 기정으로는 no이다.

ARCnet지원? 이 선택은 ISDN 광지역망기판지원을 가능하게 한다. ISDN리용을 계획한다면 또한 이미 설명한 PPP지원도 유효로 하여야 한다. 기정으로는 모듈지원이다.

동기식PPP지원? 이 선택은 ISDN회선에서 동기식통신을 지원한다. 일부 ISDN하드웨어는 이 선택을 유효로 할것을 요구하며 련결시에 이 리용을 협의한다. ISDN을 리용하려면 필요한 경우에 이 선택을 유효로 하여야 한다. 기정으로는 Yes이다.

동기식PPP에서 VJ-압축리용? 이 선택은 동기식PPP가 리용될 때 머리부압축을 가능하게 한다. 기정은 Yes이다.

일반 MP(RFC 1717)지원? 동기식PPP가 리용될 때 이 선택은 ISDN회선에서 다중통신을 가능하게 한다. 이 선택은 새로운 규정으로서 아직 광범히 지원되지는 않는다. 기정으로는 no이다.

ISDN에서 음성지원? ISDN기판이 지원될 때 이 선택은 Linux체계가 수신되는 음성호출을 접수하고 응답할수 있게 있다. 기정으로는 no이다.

NFS파일체계지원? 이 선택은 NFS를 리용한 파일체계의 설치와 봉사를 지원할수

있게 한다. NFS는 UNIX체계들사이 파일을 공유하는데 가장 많이 사용된 다. 또한 다른 플래트홈에 의해서도 지원된다. 기정으로는 Yes이다.

SMB파일체계지원? 이 선택은 NetBIOS/NetBEUI공유를 지원하게 할수 있다. SMB는 Microsoft의 Windows체계에서 파일과 인쇄기공유를 위하여 가장 많이 사용된다. 기정으로는 Yes이다.

SMB Win 95오유작업? 이 선택은 Linux체계가 파일을 공유하고 있는 Windows 95체계의 등록부정보를 회복하려고 시도할 때 일부 련결문제들을 고정시킨다. 기정으로는 no이다. Windows 95가 공유한 파일을 리용한다면 이 설정을 유효로 하여야 한다.

NCP파일체계지원? 이 선택은 Linux체계를 NetWare봉사기에 련결할수 있게 한다. 련결되면 Linux체계는 NetWare봉사기의 파일체계를 설치할수 있다. 기정으로는 모듈지원이다.

의존성검사

구성선택을 끝낸 다음에는 make dep를 기동시킨다. 이 지령은 핵심부를 콤파일하기 전에 의존성검사를 실행하여 요구되는 모든 파일들이 존재하는가를 확인한다. 체계속도에 따라 이 지령실행은 1~15min 걸린다. 초원을 바라보는것처럼 시원한 느낌은 없지만 오유가 없다는것을 확인하기 위하여서는 주의를 집중하여 의존성검사를 정확히 하여야 한다.

일러두기

오유는 보통 필요한 파일을 빠뜨린것으로 하여 발생한다. 무엇이 빠졌는가를 알면 전 단계들을 조사하면서 어느 단계에서 잘못하였는가를 찾아 낼수 있다.

작업공간지우기

다음은 모든 대상파일들이 제거되였는가를 확인하기 위하여 make clean을 실행할수 있다. 이것은 최신개정판핵심부들에서는 대체로 요구되지 않지만 실행시킬 때 파괴되는 것은 없다. 이 지령은 보통 1min이내에 실행된다.

핵심부콤파일

현재까지 기존능동체계를 변경시키지는 않았다. 모든 변경들은 파일들을 구성한것뿐이다. 다음지령 make zImage는 선택한 구성파라메터들에 기초하여 핵심부를 창조하여 현재 리용하고 있는 핵심부를 교체한다. 핵심부가 너무 크다(2.2.x이상의 핵심부들에서는 공통적이다.)는 오유가 발생하면 make bzImage를 리용하여 압축형태로 핵심부를 창조한다.

주 의

zImage와 bzImage에서 I가 대문자이라는것을 명심해 두기를 바란다. 왜냐하면 UNIX체계가 대문자와 소문자를 엄격히 구별하기때문이다.

이 지령은 처리기속도와 체계에 실장한 물리기억의 크기에 따라서 실행시간이 좌우되지만 다른 지령에 비하여 오랜 시간이 요구된다. 주기억 128MB, 400MHz인 펜티움에서 새로운 핵심부를 창조하는데 10~20min간 걸린다.

기동관리자구성하기

다음단계는 새로운 핵심부에 대한 지시기를 설정하는데 필요한 Linux기동관리자 LILO를 만드는것이다. 이것은 지령 make zlilo, make bzlilo를 실행하든가 또는 /boot등록부에 핵심부를 복사하고 수동으로 /etc/lilo.config를 만들 때 새로운 핵심부에 대한 입구점들을 추가한 다음 lilo지령을 재기동하여 진행된다.

이제는 체계를 재기동하면 새로운 핵심부으로부터 기동한다. 체계기동시에 새로운 오유에 대하여 주목할 필요는 없다. 체계기동이 완전히 거절되면 비상회복디스크를 리용하여 체계를 재기동하고 이 장의 《핵심부구성하기》절에서 설명한 여벌핵심부를 재적재한다. 이것은 체계를 재기동하여 무엇이 잘못되였는가를 찾을수 있게 한다.

망구동기설정의 변경

망구동기의 구성에서 오유가 나타나면 망구동기설정을 변경하여야 한다. 이것은 Real Hat의 조종탁에서 핵심부데몬구성선택으로 진행된다. 그림 15-4에 장치구동기의 설정을 추가, 제거, 변경할수 있는 핵심부구성창문을 보여 준다.

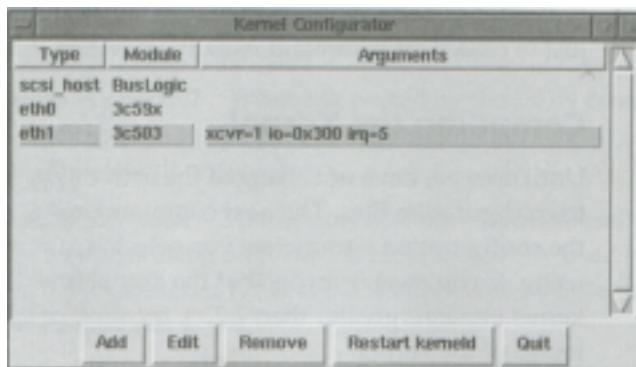



그림 15-4. 핵심부구성창문

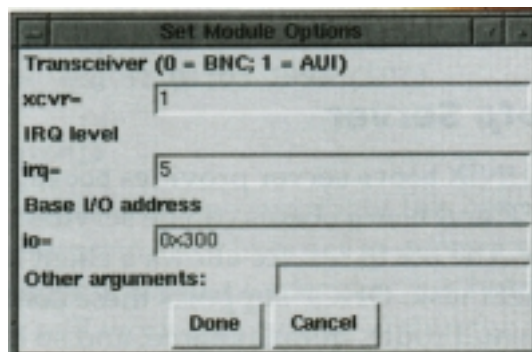



그림 15-5. 특정구동기에 대한 기동파라메터들을 변경할수 있는 모듈선택설정창문

특정한 구동기를 지정하고 Edit를 선택하면 그림 15-5에 보여 준 모듈선택설정대화칸이 나타난다. 여기서는 Linux가 망기판을 초기화할 때 리용하는 구성파라메터들을 변경할수 있다. 변경이 끝나면 유효로 하기 위하여 핵심부를 재기동할수 있다.

핵심부를 창조하는데서는 반드시 리용하려는 선택들만 지원하도록 핵심부를 최적화하여야 한다. 이것은 지원을 핵심부자체에서 제거하기때문에 공격자가 임의의 봉사에 접근하는것을 차단할수 있다. 공격자가 봉사에 접근하기 위하여 어떤 기능을 지원하자면 체계핵심부를 재구축하여야 한다. 그러므로 이러한 문제들이 무시되지 않도록 핵심부를 최적화하는것이 제일 좋다.

일러두기

일단 핵심부를 최적화하였다면 다음은 불필요한 IP봉사들을 제거하여야 한다.

IP봉사관리

UNIX는 많은 IP봉사를 지원할수 있는 체계로 발전하였다. 이것은 기능상 측면에서는 아주 우수하지만 보안상측면에서는 그렇지 못하다. 봉사가 다양한 체계는 취약성이 로출될 가능성이 더 크기때문에 쉽게 리용당할수 있다. 실례로 UNIX체계를 공격하려는 공격자들은 HTTP, FTP, SMTP봉사들에서 엄격한 보안대책이 강구되였지만 고려하지 못한 결점들이 있다는것을 알아 내려고 시도한다.

다음의 몇개 단락들에서 UNIX에서 특징적인 IP봉사들과 불필요한 점들을 어떻게 제거하는가에 대하여 설명한다.

IP봉사

UNIX에서 가능한 IP봉사들은 대단히 많다. UNIX의 특징은 기정으로 어느 봉사가 유효인가를 결정할수 있다는것이다. 그러므로 어느 봉사가 동작하고 있는지를 확인하기 위하여 봉사와 관련한 구성정보를 검사할 필요가 있다. UNIX에서 공통적으로 유효한 봉사들은 다음과 같다.

bootp봉사기

UNIX의 bootp봉사기는 망의뢰기들에 기동관련규약(bootp)과 동적호스트구성규약(DHCP)봉사를 제공한다. DHCP와 bootp의뢰기들은 독자적으로 또는 복합환경에서는 서로 련관되여서 봉사를 제공 받을수 있다. bootp봉사는 의뢰기가 동적으로 IP주소와 부분망마스크정보를 얻을수 있게 한다. DHCP는 이러한 구성설정과 기정경로, 령역이름 등과 같은 많은 정보제공을 지원한다. 대부분 UNIX체계들은 bootp봉사기를 기동하지 않는다.

DNS봉사기

UNIX플래트홈을 위하여 선정된 령역이름봉사기는 버클리 인터네트이름 령역(BIND)봉사기이다. BIND는 인터네트에서 령역이름정보교환에 리용된 최초의 그리고 여전히 광

범히 리용되는 도구프로그람이다. BIND봉사기는 1차, 2차 또는 완충기능만을 가진 령역이름봉사를 제공할수 있게 구성될수 있다.

대부분의 UNIX조작체계는 국부DNS봉사기를 기동한다. BIND는 1차 또는 2차로 동작하도록 체계를 구성하지 않는 한 기정으로는 완충이름봉사기로 동작하도록 구성되여 있다. BIND는 완충이름봉사기로 동작할 때에는 TCP와 UDP포구 53에 대한 문의에만 응답할수 있다. BIND는 named라는 자기자체의 개별적인 처리로서 동작한다.

BIND는 해커들이 UNIX체계 접근을 위하여 자주 리용하고 있는것으로 하여 이름이 났다. 그러므로 BIND의 최신판본을 구입했는가를 확인하고 중요한 망봉사에 관해서는 최신보안정보문제들을 CERT(www.cert.org)와 검사하여야 한다.

Finger봉사기

특정콤퓨터의 사용자정보를 볼수 있는 UNIX의 기능인 Finger는 보안을 위하여 리용되지만 중요한 보안구멍을 제공할수 있는 봉사기들중의 하나이다.

UNIX는 의뢰기와 봉사기에 대한 Finger봉사를 제공한다. 이 봉사는 사용자에 대한 정보를 조사할수 있도록 이름에 따라 구좌정보를 제시한다. Finger요구로부터의 출력실례를 아래에 보여 준다.

```
[cbrenton@thor cbrenton]$ finger root@loki.foobar.com
Login:root                    Name:root
Directory: /root                     Shell: /bin/bash
Last login Sun Aug 30 17:43 (EDT) on ttyp0 from 192.168.1.25
New mail received Mon Aug 31 02:41 1998 (EDT)
      Unread since Mon Aug 31 01:03 1998 (EDT)
No Plan.
[cbrenton@thor cbrenton]$
```

이 출력에는 주목할만 한 가치가 있는 몇가지 점들이 있다. 우선 Loki라는 원격기계의 어떤 사용자를 문의하기 위하여 체계 Thor로부터 Finger의뢰기를 기동하고 있다. Finger는 국부접근만이 아니라 망상의 리용을 위해서도 설계되였다. 또한 Finger는 뿌리사용자를 포함하여 passwd파일에 있는 임의의 사용자와 작업한다.

우의 출력실례로부터 뿌리사용자가 192.168.1.25에서 telnet대화(ttyp0)를 통하여 련결하였으며 토요일부터는 체계를 검사하지 않았다는것을 알수 있다. 만일 이 체계에 대한 공격을 계획하고 있다면 우의 실례로부터 중요한 정보를 가질수 있게 된다.

- 검사를 피하기 위한 정보로서 뿌리가 체계를 어떤 주기로 검사하는가를 알아낼수 있다.
- 뿌리가입을 위한 통과암호를 얻기 위하여 Loki와 192.168.1.25사이의 telnet대화를 감시할수 있다.
- 일단 뿌리의 통과암호를 얻으면 뿌리가 telnet를 통하여 인증될수 있기때문에 기계에 대한 물리적접근이 필요 없다는것을 안다.

이것은 단순히 하나의 지령을 기동하여 얻은 아주 많은 량의 정보이다. 뿌리사용자가 실지로 체계에 련결하였을 때 류사하게 다음의 결과가 나타났다고 하자.

```
[cbrenton@thor /etc]$ finger deb
Login:deb                              Name: Deb Tuttle
Directory: /home/deb                   Shell: bin/bash
On since Mon Aug 31 13:15 (DET) on ttyp3 from 192.168.1.32
 16 minutes 46 seconds idle
No mail
No Plan
```

여기서 알수 있는바와 같이 Deb는 192.168.1.32에서 telnet대화를 능동으로 유지하고 있었지만 16min 42s동안 아무것도 하지 않았다. 만일 누가 Deb의 콤퓨터에 물리적인 접근을 할수 있다면 Deb가 자기의 위치를 리탈했다는것을 의미하는 비활동시간을 리용할수 있다. 이것은 다른 사람이 Deb의 콤퓨터에 있는 어떤 흥미 있는 자료를 볼수 있는 커다란 가능성을 조성한다.

Finger는 이 장에서 후에 설명하는 inetd아래의 처리로서 동작한다. 대부분의 UNIX는 기정으로 Finger를 유효로 설정하고 있다.

FTP봉사기

UNIX는 익명FTP봉사를 포함한 FTP봉사를 제공한다. 체계련결을 위하여 유효한 가입이름과 통과암호로 FTP를 리용하면 자기의 홈등록부로 떨어 지며 파일체계에 대한 보통준위의 접근을 가지게 된다.

그러나 anonymous가입이름을 리용하여 인증되면 부분등록부(대체로/home/ftp)로 떨어지며 이 점우의 등록부들은 볼수 없다. 익명 FTP사용자에 한해서는 /home/ftp가 뿌리준위 등록부로 된다.

주　의

/home/ftp임의의 부분등록부설정은 익명사용자가 파일에 대한 읽기 또는 읽기쓰기접근을 가질수 있게 한다. 이것을 익명 FTP접근이라고 하며 사용자들이 적당한 인증없이는 전체 파일체계에 접근하지 못하게 한다.

FTP는 inetd아래의 처리로서 동작한다. 대부분의 UNIX판들은 FTP봉사기를 기동하지만 모든 익명FTP접근은 지원하지 않는다. 가장 대중화된 FTP인 wu-ftp는 해커들이 체계에 침투할수 있는 결점을 가지고 있는것으로 하여 유명하다. DNS와 같이 안전한 최신 판본을 구입하며 기동하고 있는 FTP판에 알려 진 결점들이 없다는것을 CRET와 확인하여야 한다.

HTTP봉사기

많은 UNIX체계들이 아파치(Apache)라는 Web봉사기(현재까지는 가장 대중화된 Web봉사기이다.)를 기동한다. 아파치는 Java스크립트기능과 여러 홈기능(multihoming)과 같은 개선된 기능들을 지원하기때문에 UNIX기반Web봉사기들중에서 우세를 차지한다. 여러 홈기능은 같은 Web봉시기에 여러개의 령역이름을 가지게 하는 기능이다. 아파치는 목적지Web봉사기를 찾고 그 령역에 해당한 적당한 등록부구조로 문의를 보낸다.

HTTP는 이전의 축적CGI스크립트들에서 취약성이 발견되였기때문에 가동을 포기하는것으로 하여 특별히 불쾌한 처리이다. 만일 봉사기를 능동으로 계속 유지하고 있다면 아마 많은 이전 스크립트들을 이미 갱신하였을것이다. 이러한 문제들을 피하기 위하여서는 체계에 적재되여 있으면서도 주의를 돌리지 않았던 HTTP처리들을 제거하는것이다. Web봉사는 httpd라는 자기자체의 개별적인 처리로 동작한다.

IMAP와 POP3봉사기

UNIX는 POP과 IMAP를 리용하여 원격우편검색을 지원한다. POP3은 이전시기의 표준으로서 대부분 원격우편의뢰기들에 지원된다. IMAP은 POP3보다 더 많은 특징들을 지원하고 있다. IMAP는 현재 대중화되기 시작하였다. IMAP에는 일부 공개된 약점들이 있으므로 최신 판본을 구입하여 기동하여야 한다.

대부분 UNIX는 POP3과 IMAP봉사를 능동으로 한다. 둘다 inded아래의 처리로서 동작한다.

주 의

POP3과 IMAP에 대한 더 자세한 정보는 제3장을 참고하길 바란다.

Login과 exec

이 두개의 데몬(login과 exec)을 신뢰된 호스트데몬이라고도 한다. 이것은 이 데몬들이 원격사용자가 통과암호인증을 요구함이 없이 체계에 접근할수 있게 하기때문이다.

이 데몬을 리용하는 지령은 rcp(원격체계로 파일복사), rlogin(원격체계로 가입), rsh(원격체계우에서 지령실행)이다. 이 지령들을 총괄하여 R지령이라고도 한다.

신뢰는 보안등가에 기초한다. 한 체계가 다른 체계를 신뢰할 때 이 체계는 모든 사용자들이 정확히 인증되였으며 신뢰된 체계로부터 공격이 절대로 일어 나지 않는다는것을 담보한다. 그러나 이러한 신뢰는 련쇄후과를 일으킬수 있다. 공격자는 하나의 UNIX체계를 손상시키고 그 다음은 신뢰된 호스트를 리용하여 신뢰하는 측의 체계를 손상시킨다.

신뢰된 호스트들은 letc/hosts.equiv파일의 내용에 의하여 결정된다. 이 파일에는 신뢰된 체계의 목록이 포함되여 있다. Hosts.equiv파일내용의 실례를 아래에 보여 준다.

```
loki.foobar.com
skylar.foobar.com
pheonix.foobar.com
```

이 host.equiv파일이 thor.foobar.com이라는 체계에 있다면 그때 Thor는 통파암호인증을 요구함이 없이 이 체계의 신뢰된 호스트로부터 오는 login과 exec봉사요구를 접수한다. 다른 체계가 접근을 시도하면 련결요구는 거절된다.

경　고

R지령에 의하여 제공되는 낮은 준위의 보안은 간단히 파괴될수 있다. 공격자는 통파암호보안의 약점을 리용하기 위하여 속임공격을 배비하든가 또는 가능한 DNS를 와해시킨다. 두개의 login과 exec를 inetd아래서 데몬으로 실행한다. 그러므로 이 봉사를 무효로 할것을 강하게 권고한다. 안전한 쉘(ssh)을 리용하여 같은 기능을 제공할수 있다. ssh에서는 인증과 암호화가 지원된 통신을 리용한다.

우편봉사기

대부분의 UNIX는 SMTP자료흐름을 처리하기 위하여 Sendmail을 포함한다. UNIX에서 가능한 몇개의 다른 SMTP프로그람들이 있지만 Sendmail은 가장 많이 리용된다. 이 책이 집필되는 기간에 Sendmail의 현재판 번호는 8.11.2x이였다. Sendmail의 이전 판본(특히 8.0이전)들에는 많은 부족점들이 알려 져 있다. 만일 이전 판본을 가동시키고 있다면 갱신을 진지하게 고려하여야 한다.

경　고

유감스럽게도 UNIX제작자들은 Sendmail개정을 최신판본으로 제공하지 못한다. 그러므로 새로운 OS판을 설치하면 Sendmail만은 1~2년이전 판본으로 제공된다.

대부분 UNIX판들은 Sendmail을 설치하고 기동시킨다. Sendmail은 자기자체의 개별적인 처리로 동작한다. 데몬의 이름은 Sendmail이다.

뉴스봉사기

제일 많이 리용하는 UNIX뉴스봉사기는 InterNetNews데몬(INND)이다. UNIX뉴스봉사기가 귀환기능을 제공하면 원격사용자들은 봉사기에 련결되여 새로운 뉴스기사를 읽고 서로 알려 줄수 있다. 귀환봉사를 제공하지 않을 때에는 봉사기는 단순히 인트라네트 토론그룹으로 리용될수 있다.

뉴스는 대부분 UNIX묶음에 포함되지 않는다. 이것은 전형적인 뉴스봉사기가 대체로 방대한 자원을 리용하는것과 관련된다. 대량의 디스크공간(몇주일동안의 가치 있는 기사들을 보관하는데 대체로 8GB)외에 뉴스봉사기는 가동을 위하여 낮은 등급의 처리기를 완전히 독점하여 리용한다.

일러두기

뉴스는 가동할 때 체계를 뉴스봉사만을 담당하도록 전용봉사기로 하는것이 좋다.

NFS봉사기

UNIX는 NFS를 리용하여 봉사기파일체계의 일부를 NFS의뢰기로 보내든가 또는 NFS 의뢰기자체가 원격파일체계를 탑재할수 있게 한다. 기능적으로는 원격파일체계의 일부를 구동기문자에 대응시키는 NetWare 또는 자원을 공유하는 NT봉사기와 같다. 차이는 원격 NFS파일체계가 UNIX의뢰기파일체계의 임의의 위치에 탑재할수 있다는것이다.

대부분 UNIX는 NFS 1.0판을 지원한다. NFS의 초기판은 전송규약으로 UDP를 리용하므로 아주 불안정하다. NFS 2.0판은 TCP를 지원하여 정적파케트려과기능을 리용할수 있게 되여 있다. 많은 UNIX조작체계들은 NFS봉사기를 능동으로 한다. 특별한 구성을 하지 않는한 기정으로는 파일체계를 의뢰기로 내보내지 않는다.

숙련된 해커들이 파케트려과기능을 우회하거나 람용하기때문에 NFS의 리용이 위험한 모험이라는것을 항상 생각하여야 한다. 반드시 필요한 경우에만 그것도 방화벽뒤에서만 NFS를 리용하여야 한다.

SAMBA

SAMBA는 UNIX기계가 대화통보문블로크(SMB)의뢰기 또는 봉사기로 도약할수 있게 하는 도구집합이다. 이것은 Windows체계가 리용하는 같은 규약이기도 하다. SAMBA가 동작하는 UNIX체계는 비록 PDC 또는 BDC로 동작하지는 못하지만 Windows작업그룹 또는 령역과 관계할수 있다. 다시 말하여 UNIX기계가 Windows체계와 파일 또는 인쇄기를 공유할수 있다.

대부분의 UNIX에서는 SAMBA를 미리 설치하지 않는다. 그러나 Linux는 제외이다. SAMBA는 inetd에 의하여 조종되지 않으며 자기자체의 데몬들로 동작한다. 이 데몬들은 smbd와 nmbd이다.

Talk

UNIX는 Talk를 지원한다. 이것은 인터네트중계담화(Internet Relay Chat.IRC)와 류사하다. Talk는 대화가 두 UNIX기계사이에 직접 창조되기때문에 전용봉사기를 요구하지 않는다. Talk users @ host.domain을 입력하여 련결을 설정할수 있다.

Talk요구의 응답자는 련결을 접수 또는 거절할수 있다. 일단 련결이 설정되면 화면이 입력과 출력용으로 갈라 지며 사용자들은 동시에 통보문을 입력할수 있다. 대부분의 UNIX는 Talk를 설치하고 기동시킨다. Talk는 inetd아래의 처리로 동작한다.

현대의 보안방책은 기능최소화이므로 꼭 필요할 때에만 Talk를 기동시켜야 한다. Talk와 같은 의뢰기들을 리용하면 같은 통신능력을 보존할수 있다. 일부 실례들은 IRC, ICQ, America Online's Instant Messenger(AIM)를 포함한다.

시간봉사기

UNIX는 망상에서의 시간동기화를 위하여 망시간규약(NTP)을 리용할수 있다. 망상에서 한 체계를 시간참조봉사기로 설치한다. 이 봉사는 인터네트상의 많은 시간봉사기들중 하나와 시간을 맞춘다. 그 다음 망상의 다른 체계들은 시간참조봉사기를 검사하여 자기의 체계시간을 정확히 유지한다.

대부분의 UNIX체계는 NTP를 설치하고 기동시킨다. NTP는 inetd아래의 처리로 동작한다. 최신판본인 NTP3은 망상의 참조봉사기의 식별을 위하여 증서를 리용할수 있다. 그리하여 미지 봉사기가 참조봉사기로 가장하는것을 방지한다.

주 의

NTP에 대한 직접적인 불법리용은 알려 진것이 없지만 보안방책이 완만하게 설정되여 있으면 공격자들이 가짜시간정보를 류포시키려고 시도할수 있다.

Telnet 봉사기

UNIX는 봉사기에 대한 원격조종탁접속을 제공하기 위하여 telnet요구를 접수한다. telnet를 통하여 체계와 련결한 의뢰기들은 봉사기조종탁과 같은 능력을 가질수 있다.

주 의

이것은 유력한 기능이므로 UNIX기계에 대한 telnet접근을 제한하도록 추가적인 설정을 반드시 계획하여야 한다.

telnet는 현재 모든 UNIX들에서 지원된다. 기정으로 telnet봉사는 능동이다. Telnet는 inetd아래의 처리로 동작한다.

telnet를 안전하게 하기 위하여서는 뿌리로서의 가입을 포함하여 telnet대화에서 수행될수 있는 관리자기능을 제한하든가 또는 telnet를 ssh로 교체하는것이다. ssh는 같은 기능을 제공하지만 통신을 암호화한다. 그러나 telnet에서는 사용자이름과 통과암호가 평문으로 전송된다.

Inetd

inetd는 UNIX체계에서 봉사포구감시를 책임진 상위봉사기이다.

또한 봉사요구가 수신될 때 해당한 데몬을 기동시키는 기능도 담당한다. inetd는 어떻게 봉사요구를 조절하겠는가를 결정하기 위하여 두개의 파일을 리용한다.

Services : 매 포구와 결합된 봉사를 식별한다.
inetd.conf : 매 봉사와 결합된 데몬을 식별한다.

봉사파일

봉사파일은 제3장에서 구체적으로 설명하였으므로 여기서는 간단히 개괄한다. 봉사파일은 inetd가 감시하려고 예상한 매 포구를 식별하는 단일렬입구점을 포함한다. telnet에 대한 렬입구점의 실례는 다음과 같다.

```
telnet    23/tcp    #Provide remote terminal access
```

이것은 tcp포구23으로 수신된 요구가 telnet봉사에 접근하려고 시도한다는것을 의미한

다. 사용자가 telnet에 접근하려고 한다는것을 inetd가 확인하면 이 요구를 어떻게 조절하겠는가를 결정하기 위하여 inetd.conf파일을 참조한다.

inetd.conf

inetd.conf파일에는 어느 데몬이 주어 진 봉사요구를 기동하는가를 나타내는 렬입구절들이 포함되여 있다. inetd.conf파일의 실례는 다음과 같다.

```
# These are standard services.
#
ftp      stream tcp  nowait  root  /usr/sbin/tcpd  in.ftpd −1 −a
telnet   stream tcp  nowait  root  /usr/sbin/tcpd  in.telnetd
gopher   stream tcp  nowait  root  /usr/sbin/tcpd  gn
#smtp    stream tcp  nowait  root  /usr/bin/smtpd smtpd
#nntp    stream tcp  nowait  root  /usr/sbin/tcpd in.nntpd
#
# Shell, lohin, exec and talk are BSD protocols.
#
shell    stream tcp  nowait  root  /usr/sbin/tcpd  in.rshd
login    stream tcp  nowait  root  /usr/sbin/tcpd  in.rlogind
#exec    stream tcp  nowait  root  /usr/sbin/tcpd  in. Rexecd
talk     dgram  udp  wait    root  /usr/sbin/tcpd  in. Talkd
ntalk    dgram  udp  wait    root  /usr/sbin/tcpd  in.ntalkd
#dtalk   stream tcp  waut  nobody /usr/sbin/tcpd  in.dtalkd
#
# Pop and imap mail services et al
#
pop−2 stream tcp nowait  root  /usr/sbin/tcpd   ipop2d
pop−3 stream tcp nowait  root  /usr/sbin/tcpd   ipop3d
imp   stream  tcp nowait root  /usr/sbin/tcpd   imapd
#
# Tftp  service  is  provided primarily for booting. Most sites
# run this only on machines acting as «boot servers.» Do not uncomment
# this unless you *need* it.
#
# tftp     dgram  udp  wait  root  /usr/sbin/tcpd  in.tftpd
# bootps   dgram  udp  wait  root  /usr/sbin/tcpd   bootpd
#
# Finger, systat  and netstat  give out user information which may be
# valuable to potential «system crackers.» Many sites choose to disable
# some or all of  these  services  to  improve  security
#
```

```
# cfinger is for GNU finger, which is currently not in use in RHS Linux
#
finger     stream   tcp   nowait   root    /usr/sbin/tcpd   in.finger
#cfinger   stream   tcp   nowait   guest   /usr/sbin/tcpd   in.cfingerd
#systat    stream   tcp   nowait   guest   /usr/sbin/tcpd   /bin/ps □auwwx
#netstat   stream   tcp   nowait   guest   /usr/sbin/tcpd   /bin/netstat−finet
#
# Time service is used for clock synchronization.
#
time   stream   tcp   nowait   nobody   /usr/sbin/tcpd   in.timed
time   dgram    udp   wait     nobody   /usr/sbin/tcpd   in.timed
#
# Authentication
#
auth stream tcp nowait nobody  /usr/sbin/in.identd in.identd
−1 −e −0
#
# End  of  inetd. Conf
```

매 렬입구점들은 왼쪽에서 오른쪽으로 가면서 다음의 정보들을 포함한다.

- 봉사파일에서 식별한것과 같은 봉사
- 소케트류형
- 전송규약
- 초기화에서 리용한 기발
- 이 데몬에 대한 특권을 제공하는 사용자구좌
- 요구되는 스위치를 포함한 데몬의 이름

inetd가 봉사파일을 검사하여 telnet로 봉사요구를 식별하면 inetd는 inetconf파일에 접근하여 다음의 렬을 참조한다.

```
Telnet stream tcp nowait root/user/sbin/tcpd in.telnetd
```

이것은 inetd가 /user/sbin등록부에서 뿌리준위특권을 리용한다는 스위치를 가지고 in.telnetd를 리용한 tcp데몬을 기동시킨다는것을 의미한다.

경 고

뿌리준위특권아래에서 동작하는 봉사들에 대하여서는 매우 주의하여야 한다. 왜냐하면 이러한 봉사들이 공격의 첫번째 목표이기때문이다. 뿌리준위봉사를 손상시킬수 있는 공격자는 정보를 훔칠수 있으며 또한 앞으로의 접근을 위하여 뒤문을 설치할수 있다. 이러한 원인으로 하여 많은 봉사들이 guest 또는 nobody로 기동하여 낮은 준위의 접근만을 제공한다.

inetd에 의하여 호출된 봉사를 무효화

UNIX체계를 안전하게 하는 가장 좋은 방법의 하나는 모든 불필요한 봉사를 정지시키는것이다. 체계에서 기동하고 있는 봉사가 많으면 그만큼 공격자들이 체계접근을 위한 약점을 찾기가 더 쉬워 진다.

일러두기

불필요한 봉사를 제거하는것은 또한 체계성능을 높이는 단순한 방법이다. 봉사의 개수를 줄일수록 선택된 봉사를 위하여 배당할수 있는 자원은 더 많아 진다.

inetd아래서 동작하는 봉사를 무효화시키기 위하여서는 inetd.conf파일에서 입구점시작위치에 단순히 #기호를 추가한다. 실례로 체계에 대한 telnet접근을 무효화시키려면 입구점을 다음과 같이 변경하면 된다.

```
#telnet stream tcp nowait root /user/sbin/tcpd in.telnetd
```

정지시키려는 모든 봉사들에 대하여 입구점을 무효로 변경한 다음 inetd처리를 재기동한다. 이것은 봉사가 요구하는 프로쎄스식별자를 식별하고 그것을 재기동요구에 보냄으로써 수행된다. inetd에 대한 프로쎄스식별자를 찾기 위하여서는 다음과 같이 입력한다.

```
[root@thor /etc]# ps -axlgrep inetd
  151   ? SW   0:00 (inetd)
 7177 p0 S     0:00 grep inetd
     [root@thor /etc]# kill -HUP 151
     [root@thor /etc]#
```

첫번째 지령의 ps-ax부분은 동작중인 모든 프로쎄스를 출력한다는 의미이다. 출력이 한개 화면범위를 벗어 나므로 gred지령을 리용하여 추출(l, L의 소문자)한다. Gred는 ps-ax의 출력결과를 려과하여 열쇠단어 inetd를 포함한 입구점들만이 현시되게 한다. 첫번째 입구점(프로쎄스식별자 151)은 UNIX체계에서 동작하고 있는 실제의 inetd프로세스이다. 두번째 목록결과(프로쎄스식별자 7177)는 현재 탐색을 수행하고 있는 gred지령이다.

inetd가 리용하는 프로쎄스식별자를 알아 냈으므로 재기동하여야 할 프로쎄스를 지적할수 있다. 이것은 두번째 지령에 의하여 수행된다.

kill-HUP 151.

주 의

UNIX체계에서는 이름달기규칙이 엄격하므로 지령을 정확히 입력시켜야 한다.

inetd를 재기동하면 inetd.conf파일에서 무효로 표시한 봉사의 요구들은 무시된다. telnet로 봉사포구를 지적한 요구를 발생시켜서 봉사가 무효로 되였는가를 검사할수 있다.

실례로

```
telnet thor 110
```

은 POP3봉사포구(110)와의 련결을 창조한다. 만일 POP3봉사가 무효로 되여 있으면 즉시 련결거절오유가 귀환된다.

다른 봉사와의 작업

모든 봉사가 다 inetd에 의하여 호출되지는 않는다. 실례로 BIND, Sendmail, SAMBA는 매개가 다 공통적으로 자기자체의 프로쎄스로 동작한다. HTTP도 inetd에 의하여 호출되지 않고 자기자체의 프로쎄스로 동작하는 또 다른 봉사이다.

이것은 성능상측면과 관련된것이다. 즉 봉사는 inetd에 의하여 기동할 때까지 대기하지 않는다면 요구에 더 빨리 응답할수 있다. 이러한 문제는 봉사부담이 매우 큰 체계에서 성능을 향상시킬수 있는 중요한 요인이다.

독립적인 봉사의 무효화

독립적인 봉사를 무효로 하기 위하여서는 체계기동시에 봉사의 설치가 금지되게 하여야 한다. 많은 봉사들은 설치전에 열쇠파일을 찾는다. 열쇠파일을 찾지 못하면 봉사는 기동하지 못한다. 이것은 오유를 막기 위하여 리용한다. 실례로 BIND는 기동시 파일 /etc/named.boot를 찾는다. 이 파일들을 찾지 못하면 프로쎄스는 기동이 실패한다.

기동시에 프로쎄스를 무효화하는데 리용할수 있는 방법중의 하나는 프로쎄스의 열쇠파일을 제거하든가 또는 이름을 변경하는것이다. 실례로 다음의 지령은 named.boot파일의 이름을 named.boot.old로 변경한다.

```
mv named.boot named.boot.old
```

이것은 BIND의 열쇠파일찾기를 불가능하게 하여 설치를 실패로 끝나게 한다.

또한 설치스크립트의 이름을 변경하든가 또는 무효표식을 하여 단독봉사를 무효화시킬수 있다. 실례로 Linux세계에서는 모든 프로쎄스설치 스크립트가 /ect/rc.d/init.d아래에 기억된다. 이 설치파일들에는 기동하는 프로쎄스의 이름들을 가진다. 실례로 Sendmail설치스크립트는 Sendmail.init이다. 이 파일을 Sendmail.init.old로 이름을 변경하면 Sendmail이 체계설치시에 호출되는것을 막을수 있다.

설치파일을 변경하여 모든 불필요한 데몬들을 기동하지 못하게 하였다면 체계를 재기동하든가 또는 단순히 현재프로쎄스를 정지시켜서 봉사를 금지시킬수 있다. 동작중인 처리를 정지시키기 위하여서는 inetd실례에서와 같이 ps와 grep지령을 리용한다.

그 다음 스위치없이 kill지령을 실행시킨다. 이 지령의 출력은 다음과 같이 나타날것이다.

```
[root@thor /root]# ps-axlgrep sendmail
   187  ?  S   0:00 (sendmail)
   258  p0 S   0:00 grep sendmail
[root@thor /root]# kill 187
[root@thor /root]# ps -axlgrep sendmail
   263  p0 S   0:00 grep sendmail
[root@thor /root]#
```

UNIX체계에서 기동하는 봉사의 수를 제한한 다음에는 TCP포장기를 리용하여 봉사에 접근하는 사용자수를 제한한다.

TCP포장기

TCP포장기는 어느 호스트가 inetd에 의하여 관리되는 봉사에 접근할수 있는가를 지정할수 있게 한다.

대부분의 UNIX 현재판들은 TCP포장기를 미리 설치하게 한다.

주 의

자기 이름과는 달리 TCP포장기는 전송규약으로서 TCP나 UDP를 요구하는 봉사들과 함께 리용될수 있다.

TCP포장기는 실제의 봉사데몬대신에 inetd가 TCP포장기데몬을 호출함으로써 능동으로 된다. telnet실례를 다시 참고하자.

```
telnet stream tcp nowait root /user/sbin/tcpd in.telnetd
```

inetd는 telnet데몬(in.telnetd)이 아니라 실지로 TCP포장기데몬(tcpd)을 호출하고 있다. 일단 tcpd가 호출되면 봉사요구는 접근규칙표와 비교된다. 련결이 접수할수 있으면 in.telnetd데몬으로 련결요구가 전달된다. 련결요구가 접근조종에서 실패하면 련결은 거절된다.

접근조종은 두개의 파일을 리용하여 관리된다.

Hosts.allow 어느 체계가 어떤 봉사에 접근이 허가되였는가를 정의한다.
Host.deny 어떤 봉사요구가 거절되는가를 정의한다.

원격체계에 대한 접근이 확인될 때 tcpd는 먼저 host.allow파일을 검사한다. 일치한 입구점이 없으면 tcpd는 host.deny파일을 검사한다. 두 파일의 문법은 다음과 같다.

<comma separated list of services>:<comma separated list of hosts>

유효봉사는 오직 inetd가 관리하는 봉사들만이다. 유효호스트들은 호스트이름, 령역, IP주소로 목록화될수 있다. 실례로 다음의 출력을 보자.

```
[root@thor /etc]# cat hosts.allow
pop-3 imap: ALL
ftp: .foobar.com
telnet: 192.168.1
finger: 192.168.1.25
[root@thor /etc]# cat hosts. deny
ANY:ANY
```

Hosts.allow파일은 체계에 대한 련결을 가진 모든 호스트들에 POP3과 IMAP봉사에 대한 접근을 허가한다는것을 나타낸다. 그러나 FTP봉사는 foobar.com령역안의 호스트들로 제한된다. 또한 telnet는 망부분주소가 192.168.1.0인 호스트들로 접근을 제한한다. 그리고 finger는 오직 IP주소가 192.168.1.25인 호스트만이 접근을 허가한다.

Host.deny입구점은 보안자세 《허가하지 않은것은 거절한다.》를 정의한다. 봉사요구가 수신되고 hosts.allow파일에서 일치한 입구점을 찾지 못한 경우는 이 봉사가 UNIX봉사기에 대한 원격체계접근이 허용되지 않는다는것을 의미한다.

TCP포장기는 체계에 따라 접근을 구체적으로 조화시킬수 있는 아주 우수한 방법이다. 모든 UNIX체계가 방화벽뒤에 있다고 하여도 보안강화를 위한 방어대책이 다 맞을수는 없다. TCP포장기는 방화벽을 은밀히 통과하였다고 하여도 여전히 UNIX체계접근이 거절된다는것을 담보한다.

요 약

이 장에서는 UNIX체계(또는 Linux, FreeBSD와 같이 UNIX에 기초한 체계)를 어떻게 보안하는가에 대하여 고찰하였다. 파일허가와 그것이 어떻게 파일에 대한 접근제한에 리용되는가를 설명하였다. 그리고 UNIX체계가 어떻게 인증을 처리하며 뿌리사용자구좌를 엄격히 보안하는것이 왜 중요한가에 대하여 고찰하였다. 끝으로 IP봉사와 이것에 대한 호스트접근을 어떻게 제한하는가에 대하여 고찰하였다.

다음장에서는 취약성이 어떻게 리용되며 망을 보호하자면 어떻게 하여야 하는가를 설명한다.

제16장. 공격의 해부

이 장에서는 공격자들이 망자원을 손상시키기 위하여 리용하는 공통적인 속임수들과 도구들에 대하여 고찰한다. 이것은 망을 어떻게 공격하는가 하는데 있는것이 아니라 공격자들이 흔히 망의 취약성을 어떻게 찾아 내는가를 관리자로서 알아 내자는데 있다. 여기서는 공격징후를 어떻게 식별하고 그것을 막기 위하여서는 무엇을 할수 있는가에 중점을 두고 고찰한다.

먼저 공격자가 망의 외부에서 침입을 시도한다고 가정하자. 이것은 공격자가 제한된 정보를 가지고 어떤 단계들을 거쳐서 망에 접근하는가를 보기 위해서이다. 망에 이미 접근한 합법적인 사용자는 이러한 단계들을 대부분 뛰여 넘을것이다. 제1장에서 고찰한바와 같이 망공격의 압도적부분은 망내부로부터 일어 난다. 이것은 망자원을 보안하기 위하여 취한 예방조치들이 망주위에 대하여서만 집중되지 말아야 한다는것을 의미한다.

정 보 수 집

가령 어느 한 공격자가 TV광고를 보고 자기와는 정견이 다른 어떤 대방의 망을 공격하려고 결심하였다고 하자. 문제는 공격을 어디서부터 시작하는가 하는것이다. 처음에 공격자는 대방의 령역이름조차 모르고 있다. 망을 공격하기 위하여 그는 일부 조사작업들을 하여야 한다.

Whois지령

공격자가 처음으로 할수 있는것은 InterNIC에 whois로 문의하는것이다. InterNIC는 등록된 모든 령역이름을 공개적으로 접근할수 있는 자료기지에 보관하고 있다. 이 자료기지는 whois도구프로그람을 리용하여 검색할수 있다. 공격자는 령역이름이 등록되여 있다면 기관이름으로 문의하여 그것을 찾아 낼수 있다. 실례로 CameronHunt.com이라는 기관에 대한 검색으로 다음과 같은 정보들을 얻을수 있다.

```
[granite:]$ whois CameronHunt. Com
Registrant:
Cameron Hunt (CAMERONHUNT-DOM)
   392 E. 12300 So. Ste A.
   Draper, UT 84020
   US
Domain Name : CAMERONHUNT. COM
Administrative Contact, Technical Vontact, Billing Contact:
    Hunt, Cameron(CHL150) cam@cameronhunt. Com
   10312 Bay Club Ct.
```

Tampa, FL 33607
(813)207−0363

Record last updated on 05−Apr−2000.
Record expires on 19−Jan−2002.
Record created on 19−Jan−2000.
Database last updated on 12−Feb−2001 16:21:38 EST

Domain servers in listed order:

DNS. CAMERONHUNT. COM 64.36.56.58
DNS. COPPERKNOB. COM 64.36.56.59

이 단순한 지령으로 흥미 있는 일부 정보들을 얻게 된다.

- 기관의 령역이름
- 기관의 위치
- 기관의 관리상담자
- 관리자의 전화번호와 팍스번호
- 기관안에서 유효한 부분망주소(64.36.56.0)

령역이름

기관의 령역이름은 앞으로의 정보수집에 리용되기때문에 중요하다. 이 기관과 관련된 호스트 또는 사용자는 역시 이 령역이름과 결합되여 있다. 이것은 공격자에게 앞으로의 문의를 위하여 리용할수 있는 열쇠단어를 주게 된다. 다음단계에서 공격자는 추가적인 정보들을 얻기 위하여 여기서 찾은 령역이름을 리용한다.

지리적인 위치

공격자는 우의 정보로부터 이 기관이 어디에 위치하는가를 안다. 만일 공격자가 진짜 이 망에 손해를 주든가 또는 정보를 훔치려고 한다면 림시직업을 신청하든가 또는 지어 자기의 상담봉사를 제공하려고 시도한다. 공격자는 이런 수법으로 망자원에 대한 일정한 준위의 접근을 승인 받아서 조사를 계속하려고 하든가 또는 가능하면 망에 뒤문접근을 설치하려고 한다. 이를 위하여서는 약간의 걸음이 요구된다. 망주위를 통과하는 가장 손쉬운 방법은 그 내부에 초청되여 가는것이다.

다음으로 공격자는 회사의 오물장을 뒤져서 구좌와 통과암호를 찾는다면 주소정보를 리용하여 어디로 가야 하는가를 알수 있다. 공격자는 회사의 내부정보를 얻기 위하여 오물장을 샅샅이 뒤진다. 이렇게 하여 유효한 구좌이름, 통과암호 지어는 재정정보까지 얻을수 있다. 몇년동안 많은 기관들이 재생을 위하여 종이오물을 분류하였기때문에 그러한 정보를 얻는것은 단순하였다. 이러한 수법은 유용한 정보를 훨씬 더쉽게, 더빨리 찾을수 있게 한다.

관리상담자

관리상담자는 대체로 기관망의 유지를 책임진 사람이다. 일부 경우에 관리상담자의 아래에 있는 기술상담자도 목록화되여 있다. 이것은 공격자가 심리적이면서도 공학적인 공격을 시도하려고 한다면 아주 중요한 정보일수 있다. 실례로 그는 어떤 말단사용자에게 전화를 걸어 이야기한다. 《안녕하십니까. 나는 좀전에 XX부서에 입직한 사람입니다. Smith가 봉사기에 등록된 당신의 구좌에 어떤 문제가 있기때문에 나에게 전화로 알아 보라고 부탁했습니다. 당신의 통과암호가 무엇입니까?》 만일 공격자가 이런 방법으로 대화에서 성공하면 그는 적어도 망자원에 대한 최소한의 접근을 제공하는 유효한 가입이름과 통과암호를 알게 될것이다. 이 최소한의 접근은 앞으로 완전한 관리자접근을 얻을수 있는 밑천으로 된다.

전화번호

전화번호는 앞으로의 접근을 위하여서는 좀 생소한 정보로 생각되지만 실지로 효과적으로 리용될수 있다. 대부분의 기관들은 직접내부통화(DID)라는 전화봉사를 리용한다. DID는 어떤 사람이 교환수를 거치지 않고 직접 상대방과 전화할수 있게 한다. 이 번호는 보통 블로크로 배당된다. 실례로 555-0500에서 555-0699까지는 어떤 기관에 배당된 DID 번호 블로크이다. 그러므로 공격자는 그 기관이 리용하는 매 전화번호를 쉽게 찾아 낼수 있다.

공격자는 목록화된 상담자전화번호근방에서 전화를 걸어 생활적이면서도 공학적인 공격을 시도할수 있는 직원을 찾을수 있다. 공격자는 또한 련속되는 전화번호를 검사하기 위하여 전화번호발생기(War dialer)를 설치한다. 전화번호발생기는 어떤 계렬의 전화번호를 발생하는 단순한 쏘프트웨어이다. 전화번호발생기는 콤퓨터가 어느 전화번호에 응답했는가를 조사한다. 이러한 방법으로 목록을 조사하여 공격자는 망에 침투할수 있는 전화번호를 알게 되며 나아가서는 유효구좌까지 얻을수 있다.

유효한 부분망주소

whois지령에 의하여 얻어 진 정보들중에는 DNS.CAMERONHUNT.com에 대한 IP주소입구점이 있다. 공격자는 이 호스트가 방화벽의 외부에 있는지 내부에 있는지는 알수 없으나 자기의 공격을 전개할 때 리용할수 있는 하나의 유효한 부분망주소는 알게 된다.

Nslookup지령

공격자는 다음으로 nslookup지령으로 다른 정보들을 수집하려고 한다. 공격자가 망을 공격하려고 한다면 먼저 어느 호스트를 공격하여야 하는가를 알아야 한다. Nslookup지령은 DNS봉사기에 문의하여 호스트와 IP주소정보를 얻는데 리용할수 있는 아주 좋은 도구프로그람이다.

전화번호발생기로 무엇을 찾을수 있는가?

기관들은 보통 자기의 전화가입장치에 대한 보안정형을 감시한다 실례로 1998년 봄에 유명한 취약성분석도구 SATAN을 설계한 Peter Shipley는 전화번호발생기를 리용하여 일부 지역안의 전화번호들을 체계적으로 호출하였다. 그는 아무런 인증없이 완전한 접근을 허용하는 봉사체계들을 찾아 냈다 그러한 체계들은 다음과 같다.

- 재정봉사기관을 보호하는 방화벽
- 환자등록정보를 보거나 수정하는 병원체계
- 소방차를 신속히 기동시키는 소방부서체계

이것은 극단적인 실례이지만 대체로 기관들은 자기의 사용자들에게 모뎀소유를 허용한다. 사실상 이것은 직원들에게 자기 모뎀에 대한 보안책임을 부여하는것과 같다. 그러나 많은 직원들은 그것을 담당할수 있는 자질이 부족하다.

공격자는 nslookup도구프로그람을 기동할 때 리용할 DNS에 대하여 조사한다.

```
[granite:]$ nslookup
Default Server: granite. sover. net
Address: 209.198.87.33
>
```

우의 결과로부터 nslookup이 DNS에 문의할 때 봉사기 granite.sover.net를 리용한다는것을 알수 있다. 공격자가 CAMERONHUNT.com에 대한 정보를 찾으려고 하므로 기정DNS봉사기를 whois지령의 결과에서 보여 준 두 체계들중의 하나로 변경하여야 한다.

```
> server DNS. CAMERONHUNT. COM
Default server : DNS. CAMERONHUNT. COM
Address :64.36.56.58
>
```

Nslookup도구프로그람은 CameronHunt의 DNS봉사기들중의 하나로 DNS를 지적하고 있다. 모든 문의는 granite대신에 이 체계로 보내여 진다. 공격자가 처음으로 하려는것은 지역전송이다. 지역전송은 다음의 결과에서 보는바와 같이 단일지령으로 모든 콤퓨터들과 IP주소정보들을 수집한다.

```
>ls -d CAMERONHUNT. COM > hosts. Lst
[DNS. CAMERONHUNT. COM]
Received 20 answers (0 records).
>exit
```

첫번째 지령은 DNS봉사기에 CAMERONHUNT.com령역의 유효한 모든 호스트정보를 목록화하여 그것을 hosts.lst라는 파일에 현시할것을 요구한다. 수신된 20이라는 값은 지령이 성과적으로 실행되였으며 DNS에 등록된 유효한 모든 호스트정보를 수집하였다는것을 의미한다. 물론 능동등록부에 지역파일을 보관하고 있는 Windows 2000 DNS와 같은 새로운 DNS체계들은 전송이 초기에 인증되지 않은 한 이러한 요구들을 거절한다. 보안전문가들이 평가하고 많은 DNS해커들에 의하여 실증(지어 Microsoft에서까지)된바와 같이 많은 망관리자들은 이 단순한 보안절차마저도 지키지 않고 있다. 이런 경우에 공격자는 요구한 모든 정보들을 수집할수 있다.

일러두기

DNS체계가 named.boot파일을 지원한다면 xfers지령을 리용하여 이름봉사기에서 지역전송을 수행할수 있는 사용자를 제한할수 있다. 이 지령은 이름봉사기에서 지역전송을 실행할수 있는 유일한 체계들인 IP주소목록을 보관하고 있는 named.boot파일에 따라 실행된다.

공격자는 《령역을 목록화할수 없다.》는 오유통보문을 받으면 이름봉사기에서 지역전송이 특정한 호스트들도 제한되여 있다는것을 알게 된다. 지금부터 공격자는 CameronHunt망내의 부분망들을 알기 위하여 mail, ftp, www등과 같은 공통적인 이름들로 체계적으로 시도하려고 할것이다. 공격자가 이러한 추측놀음과 같은 방법으로 매개 유효한 이름들을 식별할수 있다는 담보는 없다. 그러나 지역전송이 성공하여 아래에 보여 준 host.lst파일을 얻었다면 사정은 달라 진다.

```
[DNS. CAMERONHUNT. COM]
$ORIGIN CAMERONHUNT. COM
@               1H IN SOA       DNS             postmaster(
                                5               ; serial
                                1H              ; fefresh
                                10M             ; retry
                                1D              ; expiry
                                1H)             ; minimum
                1H IN NS        dns
                IH IN NS        206.79.230.10
                1H IN MX        5 mail
cam             1H IN CNAME     mail
ftp             1H IN CNAME     web
web             1H IN A         64.36.56.58
honeypo         1H IN A         64.36.55.57
www             1H IN A         web
```

이 파일을 통하여 매우 가치 있는 정보들을 얻을수 있다. 공격자는 공격할수 있는 2개의 유효한 IP부분망주소를 알게 된다. 이때 206.79.230.0 부분망은 whois지령이 다른 령역(exodus.net)에 있는 호스트로 목록화되였기때문에 목표가 아니다.

공격자는 또한 mail이 MX기록기의 입구점이므로 령역의 우편체계라는것을 알게 된다. 그리고 mail이 이 령역의 유일한 우편체계이므로 만일 이 하나의 호스트의 기능을 제한하면 전체 령역에 대한 우편봉사를 중단시킬수 있다는것도 알게 된다. 다음으로 Web봉사기가 FTP봉사기로 동작한다는것을 알게 된다. 공격자는 Web봉사기와 Web페지를 손상시키기 위하여 FTP봉사를 리용할수 있다. 이것은 공격자에게 중요한 정보에 침투할수 있는 가능성을 제공하여 준다.

검색엔진

검색엔진은 기관의 내부망에 대한 추가적인 정보를 수집하는 아주 좋은 방법이다. 자기 기관의 령역이름에 맞는 검색을 하여 보자. 기관이 얼마동안 직결되여 있었다면 얻어 진 방대한 정보에 놀랄것이다. 여기에는 우편통보문, 뉴스그룹우편, 내부Web봉사기로부터의 페지들이 포함된다. 물론 이것은 인터네트에서 볼수 있는 경우에 해당된다.

실례로 그림 16-1을 자세히 보자. 령역 boft.org는 모든 전자우편의 송수신을 담당한 thor.boft.org라는 우편중계국을 가진다. 외부세계와 관련하여서는 Thor가 boft.org의 유일한 우편체계이다. 그러나 이 우편의 머리부를 자세히 보면 Thor뒤에 mailgw.bofh.org라는 또 다른 은페된 우편체계가 있다는것을 알수 있다.

이 우편머리부는 내부망공격에 리용될수 있는 일부 정보들을 제공한다. 우편머리부에 있는 정보들은 다음과 같다.

```
From firewalls-owner@GreatCircle.COM  Sat Jun 15 00:54:47 1997
Received: from relay2.UU.NET (relay2.UU.NET [192.48.96.7]) by ns.ams.nexial.nl
        (8.7.4/8.7.3) with ESMTP id AAA23790 for <firewalls@ams.nexial.nl>;
        Sat, 15 Jun 1997 00:54:46 +0200 (MET DST)
Received: from miles.greatcircle.com by relay2.UU.NET with ESMTP
        (peer crosschecked as: miles.greatcircle.com [198.102.244.34])
        id QQaucy06065; Fri, 14 Jun 1997 19:08:14 -0400 (EDT)
Received: (majordom@localhost) by miles.greatcircle.com (8.7.1-lists/Lists-960417-1)
        id NAA19655 for firewalls-outgoing; Fri, 14 Jun 1997 13:24:27 -0700 (PDT)
Received: (mcb@localhost) by miles.greatcircle.com (8.7.4/Miles-951221-1) id NAA19645
        for firewalls@greatcircle.com; Fri, 14 Jun 1997 13:24:21 -0700 (PDT)
Received: from thor.bofh.org (thor.bofh.org [201.15.48.10]) by miles.greatcircle.com
        (8.7.4/Miles-951221-1) with ESMTP id FAA18598 for <firewalls@greatcircle.com>;
        Tue, 11 Jun 1997 05:12:57 -0700 (PDT)
Received: from mailgw.bofh.org (mailgw.bofh.org [201.15.50.11]) by thor.bofh.org (8.7.1/8.7.1)
        with SMTP id IAA03757; Tue, 11 Jun 1997 08:05:49 -0400
Received: from Microsoft Mail (PU Serial #1654)
From: CBrenton@bofh.org (Brenton, Chris)
To: Woolly_Attacker@hacksRus.org (Woolly)
Message-ID: <1997Jun11.081300.1654.28425@mailgw.bofh.org>
X-Mailer: Microsoft Mail via PostalUnion/SMTP for Windows NT
Mime-Version: 1.0
Content-Type: text/plain; charset="US-ASCII"
Date: Tue, 11 Jun 1997 08:12:58 -0400
Subject: RE: Attack?
Sender: firewalls-owner@GreatCircle.COM
```

그림 16-1. 전자우편머리부를 연시한 검색엔진의 결과

- 우편중계국 Thor는 Sendmail이 동작하는 UNIX체계이다(Sendmail의 판번호는 8.7.1이다.).
- 우편중계국은 IP부분망 201.15.48.0우에 있다.
- Thor뒤에 mailgw.boft.org라는 은페된 우편체계가 있다.
- Mailgw호스트는 IP부분망 201.15.50.0우에 있다.
- Mailgw호스트는 Postal Union의 교환기쏘프트웨어가 동작하는 Windows NT봉사기이다.
- 내부우편체계는 Microsoft우편이다.

단일검색엔진이 찾은 정보에는 불필요한것이 하나도 없다.

일러두기

이 문제를 극복하는 방법은 우편중계국이 외부로 나가는 모든 우편머리부정보를 떼버리는것이다. 이것은 모든 우편이 중계국자체에서 발송한것으로 보이도록 함으로써 내부망의 정보가 외부로 류출되는것을 막는다.

망의 조사

공격자가 목표에 대한 일반적인 정보들을 일부 수집하였으므로 그가 여러가지 조사를 통하여 망에서 현재 어떤 체계와 어떤 봉사가 기동하고 있는가를 알아 내는것은 시간문제이다. 공격자가 림시직업 또는 전화가입접근과 같은 다른 수단으로 방화벽을 통과하였다면 이미 그러한 정보들을 알아 냈을것이다. 공격자는 조사를 통하여 망의 경로정보지어 가능한 봉사목록까지 알수 있다.

Traceroute지령

Traceroute지령은 호스트사이 망경로를 추적하는데 리용한다. 이것은 두 호스트사이 망토막들을 문서화하려는 경우에 리용할수 있다. Traceroute의 결과실례를 그림 16-2에 보여 주었다.

주 의

Windows세계에서는 8문자파일이름에 적응시키기 위하여 지령이름을 tracert로 바꾸었다.

그림 16-2의 결과는 호스트이름과 원천과 목적지체계사이에 통과해야 하는 매 경로기의 IP주소를 보여 준다. 앞의 3개렬은 앞의 망토막을 통과하는데 걸린 시간을 나타낸다.

DNS에 도달하기전에 powerinternet.net우에서 몇개의 망토막은 통과하였다. 또한 몇개의 도약들은 시간초과되였고 traceroute문의에 대한 응답이 실패하였다. 이것은 련결에서의 전송속도가 느린것으로 하여 또는 장치가 이 요구들을 려과하였기때문에 발생하였을수 있다.

```
C:\>tracert dns.cameronhunt.com

Tracing route to dns.cameronhunt.com [64.36.56.58]
over a maximum of 30 hops:

  1    <10 ms    10 ms   <10 ms  172.16.21.1
  2     50 ms    50 ms    50 ms  10.252.254.154
  3     50 ms    60 ms    50 ms  10.1.1.52
  4     51 ms    50 ms    50 ms  206.113.64.2
  5     50 ms    50 ms    60 ms  500.Serial3-9.GW6.DFW9.ALTER.NET [157.130.146.65
]
  6     50 ms    50 ms    60 ms  0.so-3-0-0.XR2.DFW7.ALTER.NET [152.63.99.254]
  7     50 ms    50 ms    60 ms  190.at-1-0-0.XR2.DFW9.ALTER.NET [152.63.96.218]

  8     50 ms    50 ms    51 ms  184.ATM7-0.BR3.DFW9.ALTER.NET [152.63.100.173]
  9     50 ms    60 ms    50 ms  137.39.93.10
 10     70 ms    70 ms    80 ms  pos0-0.atl-c000.gw.epoch.net [155.229.123.129]
 11     80 ms    90 ms    90 ms  pos5-0.dcp-c000.gw.epoch.net [155.229.57.137]
 12    101 ms   110 ms   100 ms  pos11-0-0.chi-c100.gw.epoch.net [155.229.57.174]

 13    130 ms   131 ms   130 ms  seri6-1-0.den-m100.gw.epoch.net [155.229.120.246
]
 14    130 ms   130 ms   131 ms  209.101.253.74
 15    141 ms   150 ms   150 ms  207.251.150.193
 16    140 ms   150 ms   141 ms  207.251.150.198
 17     *        *        *      Request timed out.
 18    180 ms   180 ms   171 ms  node-40243839.powerinter.net [64.36.56.57]
 19    160 ms   170 ms   171 ms  node-4024383a.powerinter.net [64.36.56.58]

Trace complete.
```

그림 16-2. tracerout지령의 결과

Nslookup정보로 다시 되돌아 가보자. 공격자에게는 여전히 honeypot주소가 CameronHunt.com령역안에 위치하는지 또는 Web싸이트가 다른위치로 이동되였는가를 확인할 필요가 남아 있다.

```
C:\>tracert honeypot.cameronhunt.com

Tracing route to honeypot.cameronhunt.com [207.108.246.6]
over a maximum of 30 hops:

  1    <10 ms   <10 ms    10 ms  172.16.21.1
  2     50 ms    51 ms    50 ms  10.252.254.154
  3     50 ms    50 ms    50 ms  10.1.1.52
  4     50 ms    50 ms    50 ms  206.113.64.2
  5     50 ms    60 ms    50 ms  500.Serial3-9.GW6.DFW9.ALTER.NET [157.130.146.65
]
  6     50 ms    70 ms    50 ms  0.so-3-0-0.XR2.DFW7.ALTER.NET [152.63.99.254]
  7     50 ms    60 ms    60 ms  190.at-1-0-0.TR2.HOU7.ALTER.NET [152.63.99.90]
  8     90 ms   100 ms    90 ms  132.at-6-1-0.TR2.LAX9.ALTER.NET [152.63.4.218]
  9    101 ms   100 ms   100 ms  196.ATM6-0.XR2.LAX2.ALTER.NET [152.63.112.153]
 10    111 ms   110 ms   110 ms  194.ATM10-0-0.GW1.PHX1.ALTER.NET [146.188.249.13
3]
 11    141 ms   150 ms   150 ms  uswest-albq-gw.customer.ALTER.NET [157.130.227.1
18]
 12    141 ms   160 ms   150 ms  20.fa6-0-0.albq-cust.albq.uswest.net [207.108.24
0.221]
 13    150 ms   160 ms   161 ms  207.108.243.86
 14     *        *        *      Request timed out.
 15     *        *        *      Request timed out.
 16     *        *        *      Request timed out.
 17     *        *        *      Request timed out.
 18     *        *        *      Request timed out.
 19     *        *        *      Request timed out.
 20     *        *        *      Request timed out.
 21     *        *        *      Request timed out.
 22     *        *        *      Request timed out.
 23     *        *        *      Request timed out.
 24     *        *        *      Request timed out.
 25     *        *        *      Request timed out.
 26     *        *        *      Request timed out.
 27     *        *        *      Request timed out.
 28     *        *        *      Request timed out.
 29     *        *        *      Request timed out.
 30     *        *        *      Request timed out.

Trace complete.

C:\>
```

그림 16-3. honeypot가 유효한 호스트가 아님을 확인한 출력

이러한 검사의 결과를 그림 16-3에 보여 주었다. 그림에서 보면 추적은 마지막망에서 끝난다. 이것은 honeypot가 존재하지 않는다는것을 의미하며 따라서 공격자는 공격목표로 되는것은 오직 64.36.56.0부분망이라는것을 알게 된다.

주 의

공격자가 CameronHunt.com에 림시직업을 구하였다든가 또는 다른 수단으로 망에 접근할수 있다면 traceroute지령을 통하여 더 많은 정보를 얻을수 있다. 즉 내부IP부분망들을 문서화할수 있고 지어 경로기와 부분망련결정보까지 얻을수 있다. 호스트 몇개를 선택하고 조사함으로써 공격자는 완전한 망도표를 만들수 있다.

호스트와 봉사의 주사

호스트와 봉사의 주사는 어떤 체계가 망에서 동작하고 매 체계를 위하여 어느 포구가 열려 있는가를 문서화할수 있게 한다. 이것은 어느 체계가 공격에 취약한가를 확인하는데서 다음단계에 해당한다. 수행해야 할 단계들은 다음과 같다.

- 망에 존재하는 체계들을 찾는다.
- 매 체계에서 동작하는 봉사들을 찾는다.
- 매 봉사가 어떻게 리용할 때 취약한가를 찾아 낸다.

이 단계들은 개별적으로 수행될수 있다. 또는 이 모든 단계를 단번에 수행할수 있는 하나의 도구에 의하여 할수도 있다. 그러나 정확한 정보를 얻기 위하여서는 한번에 한 단계씩 매 단계를 조사해야 한다.

Ping주사

Ping스캐너는 부분망의 IP주소에 대한 ICMP요구를 순차적으로 보내고 응답을 대기한다. 응답이 주어 지면 스캐너는 이 주소에 능동호스트가 있다고 가정한다. 그 다음 스캐너는 응답한 체계에 대한 하나의 등록입구점을 만들고 IP주소를 호스트이름으로 변환하기 위하여 시도한다. 단순한 묶음파일 또는 스크립트파일이 여기에 리용된다. 또한 그림 16-4에 보여 준 WidPacket(이전에는 AG그룹)의 iNetTools와 같은 여러개의 그림도형도구프로그람들도 있다.

일러두기

iNetTools의 다른 특징은 IP주소를 DNS호스트이름으로 변환할수는 없지만 대신 체계의 NetBIOS이름의 찾기는 시도할수 있다는것이다. 가령 DNS봉사기에 자기의 입구점들을 가지지 않는 Windows탁상체계들이 많은 망을 주사한다면 이것은 효과적이다.

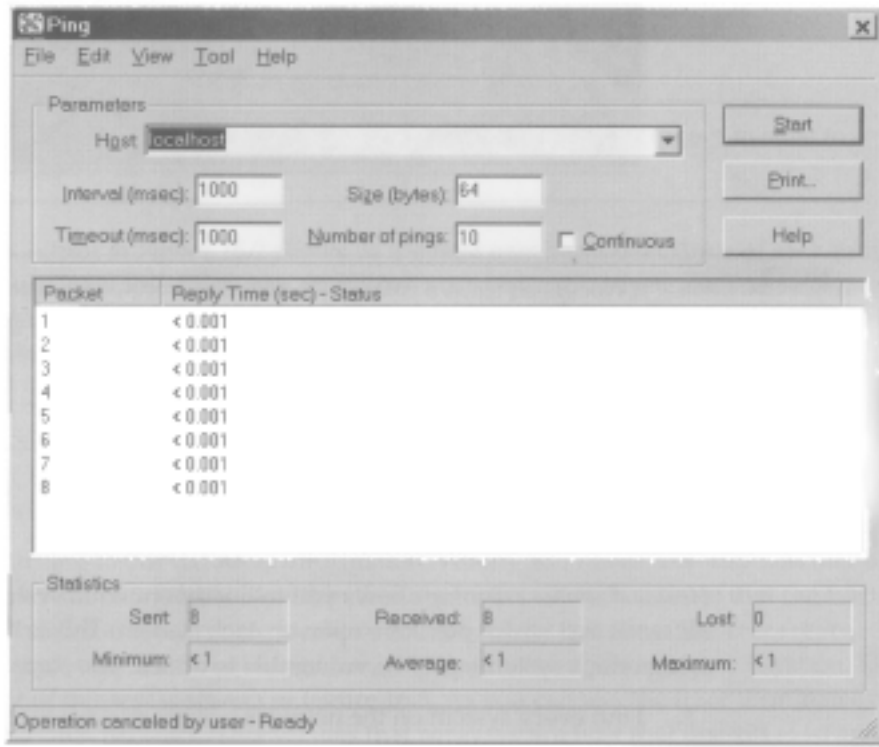



그림 16-4. iNetTools도구프로그람에 포함된 Ping스캐너

포구주사

포구스캐너를 리용하여 목적체계우의 포구번호들을 순차적으로 조사함으로써 가동중인 봉사를 알아 낼수 있다. 고층건물을 오르내리면서 문을 걸지 않았는가를 알아 보기 위하여 문손잡이를 당겨 보는 도적을 생각해 보시오. 그러면 포구스캐너가 리해될것이다. 포구스캐너는 단순히 어떤 잘 알려 진 봉사가 듣고 있으면서 련결요구를 대기하고 있는가를 식별한다.

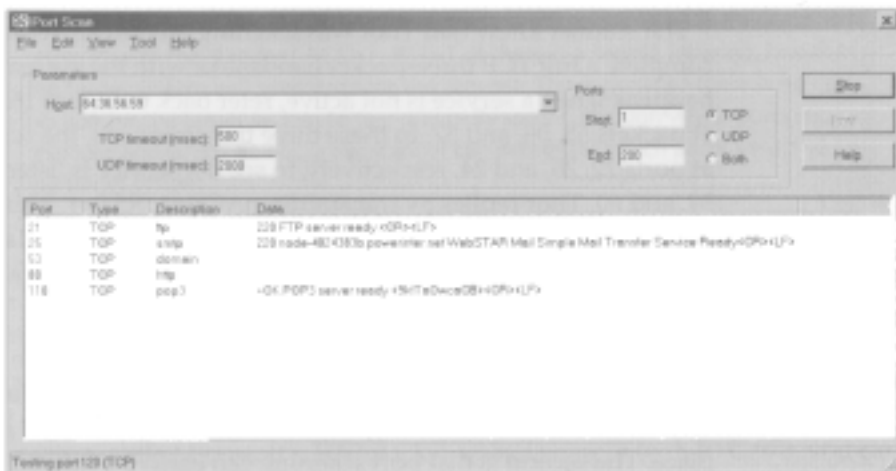



그림 16-5. 체계의 포구주사

그림 16-5는 iNetTools를 리용하여 체계 64.36.56.59를 주사한 결과를 보여 준다. 보는 바와 같이 iNetTools는 이 체계에 열려 져 있는 많은 포구들을 식별하였다. 중요한것은 열린 포구들에 대한 정보가 체계의 기능을 드러내 놓는다는것이다. 그림에서는 FTP, 전자우편, DNS, Web봉사기들이 동작하고 있다는것을 보여 주고 있다.

포구주사가 정확히 어떻게 진행되는가를 그림 16-6을 통하여 설명한다. 파케트 35를 보면 포구스캐너는 Thor라는 기계와 TCP로 3-파케트신호교환을 진행한다. 포구스캐너는 목적포구가 23(telnet)이고 SYN=1로 설정한 파케트를 전송한다. 파케트 36에서 Thor는 SYN=1, ACK=1을 전송하여 응답한다. Thor에 의한 응답이므로 포구스캐너는 telnet포구를 듣고 있는 봉사가 있다는것을 알게 된다. 파케트 37에서 스캐너는 ACK=1을 전송하여 3-파케트신호교환을 완성한다. 그다음 스캐너는 파케트 38에서 ACK=1, FIN=1을 전송하여 대화를 즉시 끝낸다. Thor는 ACK=1을 전송하여 이 요구에 응답한다.

스캐너는 체계와 완전한 TCP 3-파케트신호교환을 완성하였으므로 Thor가 포구 23을 듣고 있다는것을 알게 된다. 봉사가 정지된 경우에 포구주사가 어떻게 되는가를 보기 위하여 그림 16-6을 다시 참고하자. 이때에는 파케트 55, 56, 57을 보면 알수 있다. 이 3개의 전송에서 스캐너는 어떤 봉사가 듣고 있는지 알기 위하여 포구 22, 26, 24로 Thor를 조사하고 있다. 파케트 58, 59, 60에서 Thor는 ACK=1, RST=1을 전송하여 응답한다. 이런 방법으로 목적지체계는 이 포구에 대하여 유효한 봉사가 없다는것을 원천에게 알려 준다. 각이한 응답들을 정렬하여 포구스캐너는 어느 포구의 봉사가 기동하고 있는가를 정확히 등록할수 있다.

No.	Source	Destination	Layer	Summary	Error	Size	Interpacket Time	Absolute Time	Relative Time
35	Scanner	Thor	tcp	Port:1546 ---> TELNET SYN		64	68 ms	11:31:02 PM	2 s
36	Thor	Scanner	tcp	Port:TELNET ---> 1546 ACK SYN		64	1 ms	11:31:02 PM	2 s
37	Scanner	Thor	tcp	Port:1546 ---> TELNET ACK		64	367 µs	11:31:02 PM	2 s
38	Scanner	Thor	tcp	Port:1546 ---> TELNET ACK FIN		64	710 µs	11:31:02 PM	2 s
39	Thor	Scanner	tcp	Port:TELNET ---> 1546 ACK		64	681 µs	11:31:02 PM	2 s
40	Scanner	Thor	tcp	Port:1547 ---> 24 SYN		64	9 ms	11:31:02 PM	2 s
41	Thor	Scanner	tcp	Port:24 ---> 1547 ACK RESET		64	642 µs	11:31:02 PM	2 s
42	Scanner	Thor	tcp	Port:1545 ---> 22 SYN		64	450 ms	11:31:02 PM	3 s
43	Scanner	Thor	tcp	Port:1543 ---> FTP-DATA SYN		64	136 µs	11:31:02 PM	3 s
44	Scanner	Thor	tcp	Port:1547 ---> 24 SYN		64	69 µs	11:31:02 PM	3 s
45	Thor	Scanner	tcp	Port:22 ---> 1545 ACK RESET		64	687 µs	11:31:02 PM	3 s
46	Thor	Scanner	tcp	Port:FTP-DATA ---> 1543 ACK RESET		64	405 µs	11:31:02 PM	3 s
47	Thor	Scanner	tcp	Port:24 ---> 1547 ACK RESET		64	412 µs	11:31:02 PM	3 s
48	Scanner	Thor	tcp	Port:1548 ---> SMTP SYN		64	68 ms	11:31:02 PM	3 s
49	Thor	Scanner	tcp	Port:SMTP ---> 1548 ACK SYN		64	1 ms	11:31:02 PM	3 s
50	Scanner	Thor	tcp	Port:1548 ---> SMTP ACK		64	356 µs	11:31:02 PM	3 s
51	Scanner	Thor	tcp	Port:1548 ---> SMTP ACK FIN		64	715 µs	11:31:02 PM	3 s
52	Thor	Scanner	tcp	Port:SMTP ---> 1548 ACK		64	691 µs	11:31:02 PM	3 s
53	Scanner	Thor	tcp	Port:1549 ---> 26 SYN		64	9 ms	11:31:02 PM	3 s
54	Thor	Scanner	tcp	Port:26 ---> 1549 ACK RESET		64	653 µs	11:31:02 PM	3 s
55	Scanner	Thor	tcp	Port:1545 ---> 22 SYN		64	450 ms	11:31:03 PM	3 s
56	Scanner	Thor	tcp	Port:1549 ---> 26 SYN		64	165 µs	11:31:03 PM	3 s
57	Scanner	Thor	tcp	Port:1547 ---> 24 SYN		64	24 µs	11:31:03 PM	3 s
58	Thor	Scanner	tcp	Port:22 ---> 1545 ACK RESET		64	761 µs	11:31:03 PM	3 s
59	Thor	Scanner	tcp	Port:26 ---> 1549 ACK RESET		64	413 µs	11:31:03 PM	3 s
60	Thor	Scanner	tcp	Port:24 ---> 1547 ACK RESET		64	389 µs	11:31:03 PM	3 s

그림 16-6. TCP포구주사의 분석기출구

포구주사는 몇가지 부족점을 가지고 있다. 우선 련결시도가 목표로 한 체계에 의하여 대부분 등록된다는것이다. 이것은 목표체계의 체계관리자에게 포구주사가 있었다는것을 기록한 정보를 제공하게 된다. 다음으로 포구주사가 파케트려과 또는 방화벽에 의하여 쉽게 려과된다는것이다. 이것은 포구스캐너가 SYN=1인 초기련결파케트를 리용하기때문이다.

TCP 부분주사

TCP부분스캐너는 경과기록문제를 피하기 위하여 개발되였다. TCP부분스캐너는 완전한 TCP련결을 확립하려고 하지 않는다. 부분스캐너는 초기에 SYN=1파케트만 전송한다. 목표체계가 SYN=1, ACK=1로 응답하면 그 다음 부분스캐너는 포구가 듣고 있다는것을 알고 련결을 해제하기 위하여 즉시 RST=1을 전송한다. 완전한 련결이 실지로 확립되지 않았으므로 대부분(전부는 아니다.) 체계들은 이 주사를 등록하지 않는다. 그런데 TCP부분주사도 여전히 초기에 SYN=1인 파케트를 리용하므로 완전스캐너와 같이 파케트려파기 또는 방화벽에 의하여 차단될수 있다.

FIN주사

스캐너의 마지막류형은 FIN스캐너이다. FIN스캐너는 련결을 확립하려고 시도할 때 SYN=1인 파케트를 전송하지 않는다. 대신에 FIN스캐너는 ACK=1, FIN=1인 파케트를 전송한다. 그림 16-6에서 파케트 38을 다시 참고하면 이것이 TCP련결을 해제하기 위하여 리용되는 기발들이라는것을 기억할것이다. 사실 FIN스캐너는 련결이 존재하지 않지만 련결을 해제하려고 한다고 목표체계에 파케트를 전송하고 있다.

주 의

> 목표체계가 어떻게 응답하는가가 실지 흥미 있다. 목표포구가 봉사듣기상태가 아니면 체계는 표준절차대로 ACK=1, RST=1로 응답한다. 그러나 봉사가 듣고 있다면 목표체계는 요구를 단순히 무시해 버린다. 이것은 목표체계가 해제할 련결이 없기때문이다. 이와 같이 어느 포구가 응답으로 유도되였고 어느 포구가 그렇지 않았는가를 분석함으로써 FIN스캐너는 목표체계에서 어느 포구가 유효인가를 결정할수 있다.

이러한 류형의 스캐너가 더 파괴적인 공격을 할수 있다는것은 정적파케트려파기뿐아니라 방화벽들도 이런 류형의 주사를 막지 못하기때문이다. 이것은 공격자가 방화벽의 다른쪽에 있다고 하여도 체계를 식별할수 있는 가능성을 준다.

FIN주사는 모든 류형의 체계에 적용할수 없다. 실례로 Microsoft의 TCP탄창은 포구가 능동이라고 하여도 ACK=1, RST=1로 응답한다. 그러므로 Microsoft의 TCP탄창은 RFC973에 따르지 않는다. Microsoft체계에서는 모든 포구가 능동이 아니라는 결과가 초래되며 따라서 Windows체계에서 능동포구를 식별하는데 FIN스캐너를 리용할수 없다. 그러나 ACK=1, RST=1은 여전히 체계에 공격자가 있으며 또한 ACK=1, RST=1은 Microsoft 조작체계에 의해서도 있을수 있다는것을 알리는것으로 된다.

피동적감시

공격자는 망에 대한 더 많은 정보를 수집하기 위하여 자료흐름을 감시하려고 시도한다. 이러한 시도는 망에 어떤 분석기를 직접 설치함으로써 또는 더 위험하게는 내부체계를 식별함으로써 수행될수 있다. 즉 공격자는 자료흐름을 감시하기 위하여 망분석기를 망우에 설치하고 정보를 수집할수 있다. 이 단락에서는 내부망에 대한 정보를 수집하기 위하여 공격자들이 리용할수 있는 더 포착하기 어려운 방법들중의 하나를 고찰한다.

실례로 그림 16-7에서 파케트획득을 보자. 이것은 의뢰기가 Web봉사기에 보낸 표준 HTTP자료요구이다. 만일 공격자가 대방의 내부망사용자일부를 자기의 Web봉사기(아마 유혹적인 전자우편을 리용하여)에 접근시킬수 있다면 그는 풍부한 정보를 수집할수 있는 가능성을 가지게 된다. 왜냐하면 공격자가 파케트획득을 통하여 Web의뢰기와 원격Web봉사기사이에 교환되는 다음의 정보들을 알수 있기때문이다.

그림 16-7. HTTP 자료요구

- 선택한 언어는 영어이다
- 체계는 800×600해상도에서 동작하고 있다
- 비데오기판은 1600만개의 색을 지원한다
- 조작체계는 Windows 95이다
- 체계는 x86처리기를 리용한다
- 열람기는 Microsoft Internet Explorer3.0이다

마지막 3개의 정보는 아주 흥미 있다. 공격자는 이 체계를 공격한다면 Windows 95와 Internet Explrer3.0이 동작하고 있는 x86에 적용할수 있는 공격방법들에 초점을 두어야 한다는것을 알게 된다.

이 장뒤에서 고찰하겠지만 이러한 공격은 Internet Explorer사용자가 Web페지를 내리적재할 때 단순히 전개될수 있다.

대리방화벽이 대중화된 리유의 하나가 바로 조작체계와 열람기류형에 관한 정보를 려과한다는데 있다. 이것은 공격자들을 난처한 처지에 빠뜨린다. 즉 공격은 목표체계에 대한 정확한 약점을 쥐지 못한 상태에서 산만하게 전개된다.

주 의

망에 대하여 로출된 정보가 적으면 적을수록 공격은 훨씬 더 어려워 진다.

취약성검사

공격자가 망의 모든 체계에 대한 정보를 알고 매 체계에서 어떤 봉사가 동작하고 있는가를 알면 그 다음은 어떤 취약성을 리용하여 공격하겠는가를 찾아 내는데로 방향을 돌릴것이다. 이때 무모한 공격을 전개하여 무엇이 일어 나는가를 보는것은 모호한 양상으로 진행된다. 그러나 위험한 공격자들은 이러한 무모한 공격을 하기전에 어떤 취약성을 리용하여 공격하겠는가를 판단하는데 많은 품을 들인다. 왜냐하면 예상치 못했던 문제들로 하여 공격목적을 달성할수 없을뿐아니라 공격흔적이 기록될수 있기때문이다. 취약성검사는 수동적으로 또는 어떤 쏘프트웨어제품을 리용하여 자동적으로 진행할수도 있다.

수동적인 취약성검사

수동적인 취약성검사는 telnet와 같은 도구로 원격봉사에 련결하여 무엇이 듣고 있는가를 조사함으로써 진행할수 있다. 대부분의 봉사들은 원격호스트가 자기와 련결될 때 자기자체를 식별할수 있는 정보들을 제공한다. 이러한 정보들이 장애회복을 위한 목적에서 리용되지만 그것이 공격자들에게 더 많은 정보를 제공하는데로 리용당할수 있다.

실례로 그림 16-8을 보자. 우리는 mailsys.foobar.org에 SMTP포구로 telnet대화를 열었다. 이것은 체계지령상태에서 다음의 지령을 입력하여 수행된다.

telnet mailsys.foobar.org 25

그림 16-8. telnet를 리용한 원격우편봉사기와의 련결

마지막에 있는 25는 telnet가 기정포구 23에 련결되지 못했으며 잘 알려 진 SMTP포구 25에 련결되였다는것을 나타낸다. 여기서 알수 있는바와 같이 이 우편봉사기는 Microsoft Exchange(따라서 조작체계는 Windows NT)이며 판본은 5.0이다. 1457.7이라는 조립번호는 설치된 Exchange봉사묶음이 없다는것을 나타낸다.

조립은 초기의 5.0판본이다. 이 체계를 공격하려면 Exchange 5.0에 내재하고 있는 취

약성을 찾아야 한다. 표 16-1에 telnet를 리용하여 봉사포구에 련결할 때 리용할수 있는 지령들을 제시한다.

표 16-1 Telnet를 리용할 때 봉사포구와 관련한 지령들

봉 사	포 구	지 령	설 명
FTP	21	user, pass, stat, guit	지령대화만 제공한다. 파일을 전송할수 없다.
SMTP	25	helo, mail from:, rcpt to:, data, guit	전자우편이 이 지령을 리용하여 위조될수 있다.
HTTP	80	get	페지오유를 수신 받을수는 있지만 적어도 봉사가 능동이라는것은 알게 된다.
POP3	110	user, pass, stat, list, retr, guit	우편은 POP3포구에 련결하여 볼수 있다.
IMAP4	143	login, capability, examine, expunge, logout	모든 지령들은 유일한 렬식별자가 선행되여야 한다.

그림 16-9. telnet를 리용하여 원격IMAP4봉사기에 련결

그림 16-9는 IMAP4가 동작하고 있는 원격봉사기 Thor에 련결하기 위하여 리용된 telnet를 보여 준다. 이미 설명한 다른 봉사들과 같이 IMAP4도 통과암호를 평문으로 보낸다(cbrenton사용자의 통과암호는 2secret2이다.). 또한 IMAP4는 그림에서 1, 2, 3과 같은 렬식별자가 붙은 의뢰기들로부터 지령을 기대한다. 그림 16-8에서 알수 있는바와 같이 쏘프트웨어가 이 포구에 대한 문의에 응답하고 있다. 따라서 이 체계에 대하여 어떤 공격이 효과적인가를 식별할수 있다.

여기서 알수 있는바와 같이 수동적인 취약성검사는 약간의 작업이 필요하다. 즉 목표봉사를 확인하기 위하여 수동적인 조정이 요구되며 시간이 소비된다. 또한 수동적인

취약성검사는 공격자가 적어도 목표체계의 봉사와 관련한 단서를 어느 정도는 알아야 한다. 목표체계에서 동작하는 봉사에 대한 정보는 취약성을 어떻게 리용하는가를 잘 모르는 공격자에게도 약간의 도움이 될수 있다.

자동취약성스캐너

자동취약성스캐너는 공격자가 수동적으로 해야 하는 모든 조사와 주사단계들을 자동적으로 수행하는 단순한 쏘프트웨어프로그람이다. 이 스캐너들은 단일체계에 대하여 또는 전체 IP부분망에 대하여 진행할수 있다. 스캐너는 먼저 전개되여 잠재적인 목표들을 식별한다. 그 다음 포구주사를 진행하고 취약성을 탐지하기 위하여 모든 능동포구들을 조사한다. 그 다음 이 취약성들을 사용자에게 다시 보고한다. 프로그람에 따라서 취약성스캐너들은 자기가 찾은 취약성을 실제로 리용하는 도구까지도 포함할수 있다.

실례로 그림 16-10에서는 WebTrends의 보안분석기화면을 보여 주었다. IP부분망범위를 정의하면 이 스캐너는 그 부분망의 모든 능동체계들을 찾는다. 그 다음 포구주사를 진행하고 존재하고 있는 모든 취약성들을 보고한다. 이 프로그람은 이써네트탐지기까지 포함되여 있어 국부부분망의 자료흐름을 감시할수도 있다. 화면에서 알수 있는바와 같이 보안분석기는 IP주소가 192.168.1.200인 체계에서 포구 21과 25에 대한 잠재적인 일부 취약성들을 식별하였다.

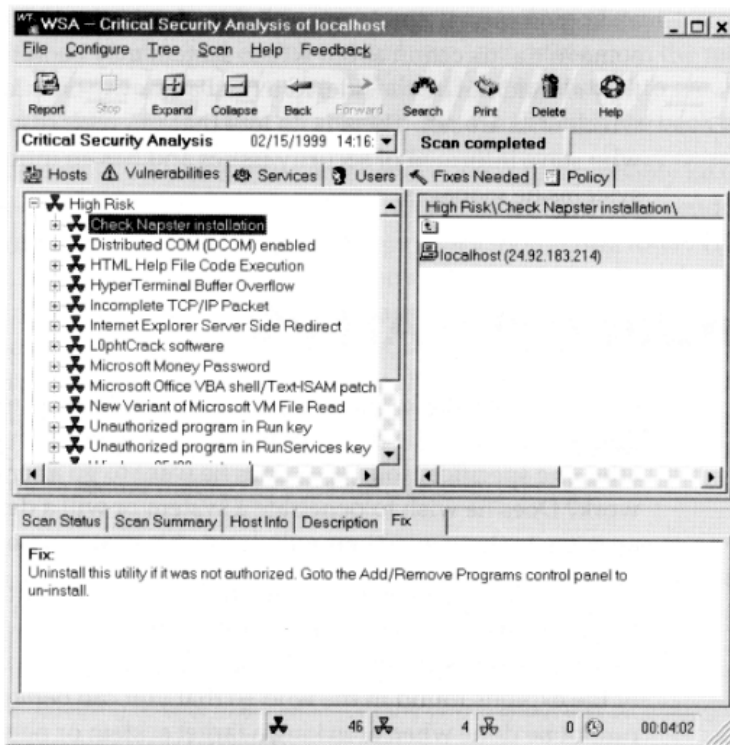



그림 16-10. WebTrend의 보안분석기

취약성스캐너는 체계에 은밀히 침입하여 문제를 식별하는 신비로운 쏘프트웨어는 아니다. 그것은 단순히 잠재적인 취약성을 식별하는 수동적인 처리들을 자동적으로 진행되게 한데 불과하다. 사실 수동적인 취약성검사를 진행하는 경험 있는 공격자 또는 해커들은 매 체계의 특성에 맞는 조사를 진행하여 잠재적인 문제들을 훨씬 더 많이 찾아 내고 있다. 취약성스캐너는 보안검열을 진행하는데서 프로그람화하는것보다는 좋지 못하다.

경 고

자동적인 취약성쏘프트웨어만을 기계적으로 동작시켜 보안검열을 하는 보안전문가들을 조심해야 한다. 그들은 대부분 쏘프트웨어묶음과 일부 여분의 값들로 만들어진 수준이 낮은 보고서를 리용하여 취약성검사를 하고 있다. 자기들이 만들어 낸 보고서를 리해하지도 못하는 그러한 전문가들이 많다. 그러므로 보안검열을 진행하기 위하여 누구와 계약하기전에 그것에 대한 참고자료들을 요구해야 한다.

실지로 원격체계에 공격을 직접 전개하지 않고 원격취약성스캐너로 모든 공격점들을 식별할수는 없다. 실례로 원격체계가 견디는가를 보기 위하여 눈물방울공격을 실제로 전개하지 않고서는 그 체계가 눈물방울공격의 영향을 받겠는가 어떤가는 론의할수 없다. 이것은 원격취약성스캐너가 어떤 특정한 문제들은 식별하지 못하기때문이다. 그러므로 정상동작을 위한 체계의 정보들을 그대로 절대적인것으로 가정하지 말아야 한다.

검사하려는 체계에서 어떤 쏘프트웨어가 동작하고 있을 때 또는 파일체계에 대한 완전접근이 가능할 때에는 공격을 전개하지 않고도 취약성스캐너로 일부 공격점들을 식별할수 있다. 그것은 국부체계에서 동작하는 쏘프트웨어프로그람들은 응용프로그람과 구동기자료들을 검사하고 목록화된 기지값들과 비교할수 있기때문이다. 실례로 검사하려는 NT봉사기에서 동작하고 있는 취약성스캐너는 tcpip.sys가 1/9/98 또는 그이후로 날자정보가 되였는가를 확인할수 있다. 이것은 눈물방울공격에 감염되지 않는 수정보충된 구동기인가를 확인할 때 사용한다.

취약성스캐너는 단순한 도구이다. 즉 알려 진 모든 보안문제들을 찾는 만능의 도구로는 되지 않는다. 취약성스캐너가 고도의 주의가 필요한 체계에 대하여 보안방향을 제시할수는 있지만 어떤 체계는 안전하고 어떤 체계는 불안전하다는데 대하여 최종적으로 결론할수는 없다. 자기가 관리하는 체계를 완전히 리해하고 있으며 보안에 대한 실천지식을 소유하고 있는 경험 있는 관리자를 대신하는 그런 도구는 아마 없을것이다.

공격의 개시

공격자가 일단 체계의 약점을 안 다음에는 공격을 전개한다. 이때 공격자가 전개하는 공격류형은 자기의 최종목적에 따라 결정된다. 즉 하나의 특정한 자원인가 아니면 망의 모든 체계자원인가 또는 체계침투인가 아니면 봉사의 거부인가에 따라 좌우된다. 이러한 목적에 따라서 공격의 다음단계가 결정된다.

여기서는 여러가지 각이한 약점들에 대하여 설명한다. 그러나 알려 진 모든 약점들을 목록화하여 설명하지는 않는다. 왜냐하면 그러한 목록은 이 책이 출판되기전에 이미 벌써 낡아 졌기때문이다. 그보다도 전혀 뜻밖에 발견된 약점실례들을 통하여 목표체계

또는 망을 공격할 때 무엇이 가능하고 무엇이 불가능한가를 리해시키는데 있다. 또한 전개될수 있는 공격류형을 미리 알고 특별한 자원이 안정한가 어떤가를 미리 결정할수 있게 하는데 있다.

주 의

이 책에서 이미 요점적으로 설명한 일부 약점들을 여기에서 구체적으로 설명한다.

숨겨 진 구좌

그자체로는 약점이 아니지만 숨은 사용자구좌는 보안방책을 완전히 회피할수 있다. 실례로 파케트려파로 망을 보호하는 주변경로기를 가지고 있다고 하자. 통과암호가 변경될수 없는 숨은 관리자준위구좌를 포함한 장치에 대하여 보안구멍을 상상해 보자. 좀 억지 같은 감은 들지만 3COM에서 있은 일을 이야기하여 보자.

1998년봄에 3COM이 자기의 CoreBuilder안에 2층과 3층준위교환기들과 숨은 관리자구좌를 가진 SuperStack Ⅱ제품계렬로 구성하고 있다는것이 드러났다. 이 장치들의 대부분에 리용된 인증인자들은 통과암호가 synnet이고 가입이름은 debug였다. 이 관리자준위구좌는 변경되거나 제거될수 없으며 관리쏘프트웨어에서도 볼수 없다. 이것은 망하드웨어를 보안할수 있는 모든 권한들을 단계별로 설정할수 있다는것을 의미한다. 그러나 공격자에게는 뒤문으로 접근할수 있는 가능성도 제공한다.

3COM은 방어에서 구좌를 펌웨어적으로 숨긴 제작자들중에서 첫번째도 아니며 마지막도 아닐것이다. 수많은 다른 하드웨어제작자들이 초기의 동기요인으로 하여 같은 지원을 제공하였을것이다. 이러한 방법은 숨은 관리자구좌를 포함시킴으로써 기술지원담당자들이 관리자통과암호를 잊어 버린 사용자들을 도와 줄수 있다는 리유로 하여 고착되였다. Cisco와 같은 많은 제작자들이 이러한 문제를 조정하는 더 안전한 방법들을 받아 들였다. 실례로 자기의 Cisco경로기에 대한 통과암호를 잊었다면 회복할수는 있지만 그때에는 장치에 물리적으로 접근할 필요가 있으며 회복처리시에는 장치를 체계와 분리시켜야 한다.

이것은 통과암호회복을 훨씬 더 안전하게 할수 있는 방법을 제공한다.

일러두기

제작자들이 어떤 일람표를 만들지 않는 한 어느 망장치에 숨은 관리자구좌가 있는가를 아는것은 불가능하다. 이것은 오직 통과암호인증에만 의거하지 말아야 하며 이러한 장치들을 보안하기 위하여서는 다른 추가적인 판정을 하여야 한다는것을 의미한다. 실례로 장치의 원격관리를 완전히 무시하든가 또는 어떤 IP주소에 대하여서만 관리상의 접근이 허용되도록 제한할수 있다.

중개자

중개자라는 약점은 파케트분석기를 리용하는 공격자가 의뢰기와 봉사기사이에 있다는것을 의미한다. 《중개자》라는 말을 들었을 때를 생각하여 보라. 대부분의 망통신이 엄격한 형태의 인증을 리용하지 않는다는 사실을 리용한 중개자공격에는 많은 형태들이

있다. 두 대화상대방들이 주기적으로 서로 확인하지 않는 한 그들은 자기가 의도한 체계가 아니라 공격자와 통신하게 될수도 있다.

대화에 대한 간섭을 보통 대화가로채기라고 한다. 공격자는 두 체계사이에 합법적인 통신대화가 시작되면 이 자료흐름에 지령들을 주입하여 상대방통신체계인것처럼 위장한다. 대화가로채기도구는 상당히 오래동안 NetWare에서 리용되였다. 임의의 사용자가 관리자의 통신대화를 가로채서 자기의 가입식별자를 관리자와 동등하게 하는 도구들도 있다. 1997년 봄에 류사한 도구가 Windows NT환경을 위하여 C2MYAZZ라는 이름으로 발표되였다.

C2MYAZZ

C2MYAZZ도구프로그람은 통신대화를 가로채기 위하여 속임수를 리용한 아주 전형적인 실례이다. Windows 95와 Windows NT가 초기에 소개되였을 때 이 체계들은 대화통보문블로크(SMB)체계와의 인증을 두가지 방법으로 실현하였다. 기정으로는 암호화된 통과암호를 리용한 인증이다. 이것은 Windows NT령역과의 인증을 위하여 적용한 방법이였다. 또한 SMB봉사기와의 뒤방향호환성을 위하여 평문통과암호를 리용한 LanMan인증도 포함하였다.

C2MYAZZ는 기동하면 의뢰기가 Windows NT봉사기에 인증되기를 피동적으로 기다린다. 가입이 검사될 때 C2MYAZZ는 대신 LanMan인증이 리용된다는것을 요구하는 하나의 파케트를 의뢰기로 전송한다. 봉사기가 이 요구를 보냈다고 믿고 있는 의뢰기는 증서를 평문으로 재전송한다. 이때 C2MYAZZ는 그것을 획득하여 가입이름과 통과암호를 현시한다. C2MYAZZ는 의뢰기의 대화를 중단시키지 않기때문에 사용자는 여전히 가입하여 체계접근을 얻을수 있다.

그림 16-11. 의뢰기가 평문통과암호를 리용하도록 하는
C2MYAZZ의 파케트획득

C2MYAZZ의 파케트획득을 그림 16-11에 보여 준다. 의뢰기는 TCP 3-파케트련결신호를 리용하여 FirstFoo라는 NT령역조종기와 련결을 확립한다. 파케트 6에서 의뢰기는 령역에 인증하려고 한다는것을 봉사기에 알린다. 파케트 7은 봉사기가 이에 대하여 응답하려한다는것을 보여 준다. C2MYAZZ가 의뢰기로 파케트를 전송했다는것을 명심하여야 한다. C2MYAZZ가 리용한 원천IP주소는 192.168.1.1로서 봉사기FirstFoo의 IP주소이다.

또한 모든 응답과 순서번호를 위조하여 의뢰기가 이 파케트를 봉사기 FirstFoo로부터 수신되였다고 가정하게 한다. 아래창은 의뢰기가 평문인증을 리용하도록 요구한 C2MYAZZ에 의하여 전송된 자료들을 보여 준다.

파케트 8에서 령역조종기 FirstFoo는 암호화가 지원된다는 응답을 의뢰기에게 보내지만 이 시점에서는 너무나 때 늦은 응답이다. 의뢰기는 이미 C2MYAZZ로부터 위장된 파케트를 받았으므로 FirstFoo가 보낸 실제의 전송을 중복으로 인정하고 정보를 페기한다. 그 다음 의뢰기는 평문인증을 위하여 가입이름과 통과암호를 둘 다 평문으로 전송하기때문에 C2MYAZZ도구프로그람은 그 정보를 그대로 리용할수 있다.

주 의

이 약점에 대하여 흥미 있는것은 봉사기와 의뢰기가 둘다 수정보충된다면 련결을 가로챌수 없다는것이다. 의뢰기는 봉사기에 인증되여 망자원접근을 허가 받는다. Microsoft는 대화가로채기와 같은 이러한 약점을 극복하기 위하여 두개의 수정보충프로그람을 개발하였다. 즉 하나는 모든 의뢰기들에 적재되고 다른 하나는 봉사기에 적재된다. 만일 의뢰기수정보충프로그람을 적재하면 의뢰기는 평문으로 가입정보를 보내기를 거절한다. 봉사기수정보충프로그람을 적재하면 봉사기는 평문가입을 접수하지 않는다. 그러므로 의뢰기가 평문인증정보를 전송하여도 봉사기는 접수하지 않는다. 그러나 매 체계들을 다 수정보충하지 않으면 C2MYAZZ에 의하여 의뢰기가 령역에 인증되지 못하여 봉사거부가 발생할수도 있다.

C2MYAZZ가 이처럼 봉사거부를 일으키는 효과적인 도구로 리용되는 리유는 의뢰기도 봉사기도 다 원격체계를 인증하기 위한 그 어떤 처리도 하지 않은데 있다. 의뢰기가 속임파케트를 합법적인것으로 접수하기때문에 C2MYAZZ는 자유롭게 대화를 가로챌수 있다. 이러한 문제에 대응하여 Microsoft는 평문인증정보의 리용을 금지시키는 수정보충프로그람을 리용하였다. 그런데 이러한 수정보충프로그람이 인증정보를 포함하지 않기때문에 SMB대화는 여전히 가로채기공격에 취약하다. 이미 설명한바와 같이 이 공격은 사용자가 관리자의 대화를 가로채서 자기의 가입식별자를 관리자와 동등하게 하는 이전 NetWare공격의 변종이다. 이것은 Novell의 파케트서명개발을 촉진시켰다.

파케트서명은 NetWare봉사기와 의뢰기가 통신대화과정에 상대방식별을 확인할수 있게 하는 인증처리이다. 봉사기가 의뢰기로부터 자료파케트를 받을 때 전송원천이 합법적이라는것을 확인하기 위하여 서명정보를 참고한다. 파케트서명은 기정으로는 다른 체계에 의하여 요구된다는 신호가 없는 한 의뢰기와 봉사기가 그것을 리용할수 없게 구성되여 있다. 이것은 인증방법으로서의 파케트서명이 기정으로는 리용되지 않는다는것을 의미한다. 지어 파케트서명이 요구되도록 의뢰기설정을 변경한다고 하여도 C2MYAZZ와 류사한 도구프로그람을 리용하여 간단히 파케트서명이 지원되지 않는것처럼 위조하여 의뢰

기에 보낼수 있다.

일러두기

파케트서명이 리용된다는것을 보증하는 유일한 방법은 고급설정으로 파케트표식을 설정하는것이다. 이것은 의뢰기가 파케트서명을 지원하지 않는 봉사기와 대화하는것을 금지시킨다.

완충기넘침

프로그람작성자가 응용프로그람을 작성할 때 사용자 또는 다른 응용프로그람으로부터 입력되는 자료를 접수하기 위하여 완충기라고 하는 기억공간을 설정하여야 한다. 실례로 가입응용프로그람은 사용자들의 가입이름과 통과암호를 입력할수 있도록 기억공간을 할당하게 한다. 이 정보를 위한 충분한 기억공간이 배치되도록 하기 위하여서는 프로그람작성자가 매 변수에 얼마만한 자료가 보관되는가에 대하여 가정을 해야 한다. 실례로 프로그람작성자는 사용자가 16문자이상의 가입이름과 10문자이상의 통과암호를 입력할 필요가 없다고 가정한다. 완충기넘침은 프로그람작성자가 예견했던 이상으로 많은 자료가 프로쎄스에 수신되여 있을 때에 발생한다. 즉 프로쎄스가 방대한 량의 자료를 취급해야 할 때 어떤 돌발적인 문제가 있어서는 안된다.

완충기넘침의 실례

완충기넘침이 어떻게 악용되는가 하는 실례를 보자. 그림 16-8에서 보여 준 telnet를 리용한 Exchange봉사기와의 대화설정을 다시 고찰하자. 만일 www.rootshell.com에 가서 Exchange에 대하여 이미 알려 진 취약성을 조사한다면 Exchange 5.0이 완충기넘침공격의 영향을 쉽게 받는다는것을 알수 있다.

실례로 사용자이름과 통과암호, 결합방법으로 구성된 LDAP결합요구를 리용할 때 256문자이상으로 결합방법을 설정하면 LDAP봉사는 기동을 멈추게 될것이며 해커가 조작한 코드를 실행할수 있다. 이것은 LDAP련결기를 프로그람화할 때 프로그람작성자결합방법을 조절하는데 254문자이면 충분하다고 가정하고 기억공간을 할당하였기때문이다. 254문자이상 되는 결합방법도 존재한다는것을 가정하는것이 안전한것 같지만 문제는 255문자로 된 결합방법을 수신하면 응용프로그람이 무엇을 해야 하는가에 대하여 프로그람작성자가 지적하지 않은데 있다.

자료를 자르던가 또는 무조건 거부할 대신에 LDAP련결기는 여전히 254문자만을 조절할수 있는 기억공간으로 이 긴 주소를 복사하려고 시도한다. 결과 254문자이후의 문자들은 다른 기억구역으로 겹쳐쓰기되든가 또는 처리를 담당한 핵심OS부분에 씌여 지게 된다. 다행히 이것이 봉사기가 기동을 멈추는것으로 끝나든가 그렇지 않은 경우에는 나머지 문자들이 조작체계의 명령으로 해석되여 이 봉사에 보증된 허가준위로 실행될것이다. 이것이 바로 뿌리 또는 관리자로서 동작하는 봉사가 위험하게 되는 리유이다. 공격자가 완충기넘침을 일으킬수 있다면 그는 자기가 목표체계에 대하여 바라던 어떤 지령들을 실행시킬수 있다.

다른 완충기넘침공격

완충기넘침은 봉사의 거부를 일으키든가 또는 원격체계에 어떤 지령을 실행시키는데서 가장 많이 적용되고 있다. 체계를 공격하기 위하여 프로쎄스에 많은 정보를 보낸다는데 기초한 공격수법들에는 여러가지가 있다. 지난 몇년동안 많이 적용된 일부 완충기넘침공격들은 다음과 같다.

- 초과크기의 ICMP요구파케트를 보낸다(죽음의 Ping).
- 4048byte의 URL요구를 IIS3.0봉사기에 보낸다.
- Netscape와 Microsoft우편의뢰기에 256문자파일이름을 부속물로 가지는 전자우편통보문을 보낸다.
- 자료크기가 정확히 정의되지 않은 SMB가입요구를 NT봉사기에 보낸다.
- Pine사용자에게 256문자를 초과하는 주소로부터 오는 전자우편을 보낸다.
- WinGate의 POP3포구에 련결하여 256문자로 된 사용자이름을 입력한다.

여기서 알수 있는바와 같이 완충기넘침은 응용프로그람의 여러가지 측면들에서 있게되며 매 조작체계에 다 영향을 미친다. 응용프로그람이 완충기넘침의 영향을 쉽게 받는가 하는것을 확실하게 알아 내는 유일한 방법은 원천코드를 다시 검사하는것이다.

주 의

완충기넘침문제를 꼬리부와 오유로부터 찾아 낼수는 있으나 여하튼 완충기넘침으로부터 생기는 오유는 쏘프트웨어가 안전하지 못하다는것을 의미한다. 그렇다고 충분한 문자수를 접수할수 있게 기억공간을 랑비할수도 없다. 프로그람이 완충기넘침의 영향을 받지 않는다는것을 확인하는 유일하게 확고한 방법은 초기원천코드를 다시 조사하는것이다.

SYN공격

SYN공격은 봉사기가 내부에로의 TCP련결을 하지 못하도록 TCP 3-파케트련결신호교환시에 리용되는 작은 완충기공간을 악용한다. 봉사기는 첫번째 SYN=1파케트를 받을 때 이 련결요구를 《프로쎄스안에서 관리하는》작은 대기렬에 보관한다. 대화가 곧 확립될 예정이므로 이 대기렬은 작으며 상대적으로 적은 수의 련결요구들만을 보관할수 있다. 이것은 대화가 곧 다른 대기렬로 이동하여 처리되므로 더 많은 련결요구들을 위한 공간이 마련되도록 기억최적화를 위하여 실현된것이다.

SYN공격은 이 작은 대기렬에서 련결요구가 초과되도록 한다. 목적체계가 응답을 발송할 때 공격체계는 그것에 아무런 응답을 하지 않는다. 결과 련결요구는 시간이 만기될때까지 상대적으로 작은 대기렬에 남아 있다가 그후에 제거된다. 이 대기렬을 가짜의 련결요구들로 채움으로써 공격체계는 목적체계가 합법적인 련결요구들을 접수하지 못하도록 차단시킬수 있다. 이와 같이 SYN공격은 봉사거부를 일으킨다.

2개의 기억공간을 리용하는것은 TCP의 표준기능이므로 이 문제를 실지로 극복하는 방법은 없다. 그러나 2가지 방법이 있다.

- 프로쎄스내부에서 관리하는 대기렬의 크기를 증가시킨다.
- 처리된 입구점들이 프로쎄스내부에서 관리하는 대기렬에서 제거되기전까지의 시간크기를 줄인다.

대기렬의 크기를 증가시켜 추가적인 기억공간을 제공하면 다른 련결요구들이 보관될수는 있지만 100MB 또는 1GB망에 련결한 체계가 SYN공격에 취약하지 않다는것을 보증하기 위하여서는 매우 방대한 크기의 완충기가 필요하게 된다. 좀 느린 망에 련결된 체계에서도 이러한 기억리용은 완전한 랑비이다. 련결요구가 제거되기전까지의 시간을 줄이는데 관하여서는 너무 느리게 계수값을 설정하면 신속한 체계들을 방해할것이고 또는 반대로 설정하면 느린 망에 련결된 체계들의 련결을 거절할것이다.

그러므로 합리적인 봉사동작을 담보하기 위하여서는 SYN공격에 피해를 받지 않도록 완충기의 기억할당을 조정하여야 한다. 완충기가 기억을 랑비하면서 크게 설정되지 않도록 하면서도 합리적인 개수만한 동시련결요구들은 조정할수 있게 프로쎄스내부에서 관리하는 대기렬의 크기를 증가시켜야 한다. 또한 제거시간을 처리된 입구점들을 제거할수 있게 충분히 크게 하면서도 합법적인 체계의 련결확립을 방해하지 않도록 적당히 설정해야 한다.

유감스럽게도 대부분조작체계들에서는 사용자가 이러한 값을 조정할수 없게 되여 있다. 그러므로 적당한 설정을 선정하기 위하여서는 조작체계제작자들에 의존하여야 한다.

눈물방울공격

눈물방울공격이 어떻게 체계에 가해 지는가를 리해하기 위하여서는 먼저 IP머리부안에 있는 토막화변위부마당과 길이마당을 리해하여야 한다. 토막화변위부마당은 대체로 경로기에 의하여 리용된다. 경로기가 수신한 파케트가 송신해야 할 다음토막에서의 최대전송단위(MTU)보다 큰 경우에는 중계하기전에 토막화를 진행하여야 한다. 토막화변위부마당은 길이마당과 함께 리용되여 수신체계가 데타그람을 정확한 순서대로 재조립할수 있게 한다. 토막화변위부값이 0인 파케트를 수신한 체계는 이 파케트가 토막화된 정보의 첫번째이든가 또는 토막화가 리용되지 않은것으로 가정한다.

토막화가 진행되였다면 수신체계는 자료가 재구성될 때 어느 파케트에 놓였는가를 결정하기 위하여 변위부를 리용한다. 설명을 위하여 아이들의 놀이감으로 리용하는 번호가 새겨 진 블로크들을 생각하자. 아이들은 번호순서에 따라서 블로크들을 놓고 집, 승용차, 비행기를 만든다. 사실 아이들은 자기들이 무엇을 만들려고 하는가에 대해서는 알 필요가 없다. 단순히 놀이감을 규정된 순서대로 조립하면 집이라든가 승용차가 만들어 진다.

IP토막화변위부도 같은 방식으로 처리된다. 변위부는 유효자료가 데타그람의 시작에서부터 얼마나 떨어 졌는가를 나타낸다. 만일 모든 파케트가 정확히 도착하면 데타그람이 정확한 순서대로 재조립될수 있다. 길이마당은 자료가 중복되지 않고 정확히 토막화되였다는것을 확인하기 위한 타당성검사에 리용된다. 실례로 데타그람안에 토막 1과 3은 배치하였으나 토막 2가 너무 커서 토막 3과 일부가 겹치게 되는 경우 어떻게 하여야 하

는가? 이때 체계가 그것을 맞출수 있는가를 보기 위하여서는 데타그람의 재편성을 시도한다. 만일 맞출수 없다면 수신체계는 자료가 완전하지 못하다는 오유통보문을 내보낸다. 대부분의 IP탄창은 중복 또는 자기 토막보다 훨씬 큰 유효자료와 관련한 상세한 처리기능을 제공한다.

눈물방울공격의 개시

눈물방울공격은 보통크기의 유효자료와 토막화변위부가 0인 일반자료파케트를 보내는것으로부터 시작한다. 초기의 자료파케트로부터는 눈물방울공격과 일반자료전송을 구별할수 없다. 그러나 부분순서화된 다음파케트들에서는 토막화변위부와 길이마당들이 수정되여 있다. 뒤이어 일어 나는 이러한 자료흐름은 목표체계가 기동을 정지하게 만든다.

자료의 두번째 파케트가 수신될 때 토막변위부는 데타그람안에서 이 정보가 어디에 놓이는가를 알기 위하여 참고된다. 눈물방울공격에서는 두번째 파케트의 변위부로 이 정보가 첫번째 토막의 어딘가 놓인다고 요구한다. 수신체계는 유효마당이 검사될 때 이 자료가 첫번째 토막의 끝을 초과하리만큼 그렇게 크지 않다는것을 알게 된다. 다시 말하여 이 두번째 토막은 첫번째 토막과 중복되지 않았다. 즉 실지로는 자기의 토막내에 완전히 포함되여 있다. 이러한 상황히 누구도 예견할수 없는 오유조건이며 그것을 조정하는 처리부분도 없기때문에 이 정보는 완충기넘침을 일으키고 수신체계의 기동을 정지시킨다. 일부 조작체계들에서는 하나의 변형된 파케트에 의해서도 정지된다. 다른 체계들에서는 여러개의 변형된 파케트들이 수신되는 경우에 체계정지가 일어 난다.

스머프

이 공격이 전개된 초기프로그람에 붙여 진 스머프(Smurf)는 IP속임과 ICMP응답의 결합을 리용하여 호스트에 자료흐름을 포화시켜서 봉사거부가 일어 나도록 한다. 공격은 다음과 같이 진행된다. 공격자는 먼저 많은 호스트들이 포함되여 있으면서 큰 대역너비를 가진 인터네트련결을 가지고 있는 망의 방송주소로 속임Ping파케트(echo요구)를 보낸다. 이러한 망은 바운스싸이트라고 한다. 속임Ping파케트는 공격자가 공격하려고 하는 체계의 원천주소를 가진다.

공격의 전제는 경로기가 IP방송주소(실례로 206.121.73.255)로 보낸 파케트를 수신하였을 때 이것을 망방송으로 인식하고 이써네트방송주소 FF:FF:FF:FF:FF:FF로 넘긴다는것이다. 그리하여 인터네트로부터 이 파케트를 수신한 다른 경로기들은 자기의 국부토막에 있는 모든 호스트들에 이것을 다시 전송한다.

독자들은 다음에 무엇이 일어 난다는것을 리해하였으리라고 생각한다. 토막우에 있는 모든 호스트들은 공격자가 공격하려는 체계에 echo응답으로 반응한다. 만일 큰 이써네트토막인 경우 500개이상의 호스트들이 자기들이 수신한 매 ehco요구에 응답할것이다.

대부분의 체계들은 ICMP자료흐름을 가능한 신속히 조종하기때문에 공격자가 목표로 한 체계는 곧 echo응답으로 포화된다. 이것은 체계가 그 어떤 다른 자료흐름도 받아 들일수 없게 방해하여 결국은 봉사거부를 일으키게 한다.

이것은 목표체계뿐아니라 기관의 인터네트련결에도 영향을 미친다. 바운스싸이트는

T3련결(45Mbps)을 가지지만 목표체계의 기관은 임대선(56Kbps)만을 가지므로 기관으로 들어 오고 나가는 모든 통신이 마비되여 거의 정지상태에 빠진다.

그러면 이러한 류형의 공격을 어떻게 막을수 있는가? 원천싸이트와 바운스싸이트, 목표싸이트들에 스머프공격의 영향을 제한시키도록 여러가지 대책들을 취하여야 한다.

원천에서 스머프차단

스머프는 공격자가 속임원천주소로 echo요구를 전송한다는데 기초한다. 자기의 원천에서 일어 나는 스머프공격은 경로기접근목록을 리용하여 모든 자료흐름이 정확히 자기의 원천주소를 가지도록 함으로써 막을수 있다. 이것은 속임파케트가 발생지로부터 바운스싸이트로 전달되지 못하도록 차단한다.

바운스싸이트에서 스머프차단

바운스싸이트에서 스머프를 막는데는 두가지 수법이 적용된다. 하나는 단순히 내부에로의 echo요구를 모두 차단하는것이다. 즉 이러한 파케트들이 망내부에 도달하지 못하도록 차단한다.

다른 수법은 경로기가 망방송주소로 예정된 자료흐름에 대하여 국부망방송주소로 변환하지 않도록 하는것이다. 이러한 변환을 금지시킴으로써 echo요구가 국부망으로 송신되지 못하도록 한다.

Cisco경로기가 망방송주소를 국부망방송주소로 변환하는것을 차단하기 위하여서는 망대면부의 구성방식을 다음의 지령으로 변경하면 된다.

No ip directed−broadcast

주 의

변경은 매 경로기의 모든 망대면부에 대하여 진행하여야 한다. 이 지령을 주변경로기에 대하여서만 진행하면 효과적이라고 볼수 없다.

목표싸이트에서 스머프차단

인터네트봉사제공자(ISP)가 도와 나서지 않는다면 WAN련결우에서의 스머프공격을 차단하기 위하여 할수 있는 일은 극히 적다. 망주변에서 이러한 자료흐름을 막을수 있다고 하여도 모든 WAN대역너비를 차지한 이 공격을 막는다는것을 너무 때 늦은 시도라고 해야 할것이다.

그러나 망주변에서 차단하여 스머프의 영향을 최소화할수는 있다. 상태를 유지할수 있는 일부 방화벽들 또는 동적파케트려과기를 리용하여 망으로 들어 오는 이 파케트들을 차단할수 있다. 상태표가 공격대화가 국부망에서 일어 나지 않는다(처음의 echo요구를 보여 주는 입구점이 상태표에 없다.)는것을 알려 줄수 있기때문에 이 공격은 다른 속임공격과 같이 조정될수 있으며 즉시에 제거될수 있다.

힘내기공격

힘내기공격이란 가능한 모든 값들로 시도하여 체계에 인증되려고 할 때 또는 암호문을 만들 때 리용한 암호열쇠를 풀기 위하여 진행하는 공격류형을 말한다. 실례로 공격자는 가능한 통과암호들로 목록화된 단어사전을 리용하여 체계에 관리자로 가입하려고 시도한다. 여기에는 그 어떤 정확성도 없다. 즉 공격자는 단순히 가능한 통과암호를 찾아내기 위하여 매 가능한 단어 또는 문구들로 시도할뿐이다.

힘내기공격에서 가장 보편적으로 쓰이는 방법들중의 하나가 통과암호해득기를 리용한 방법이다. 통과암호해득기는 보안쏘프트웨어기술의 L0phtCrack(후에 @stake로 된 L0pht에 의하여 개발)와 같이 이 프로그람이 얼마나 효과적인가를 보여 주는 그런 프로그람은 아니다. L0phtCrack는 사용자통과암호를 알아 내기 위하여 사전파일과 힘내기추측공격을 리용한다. 그림 16-12에 여러개의 사용자통과암호들을 풀기 위하여 시도한 L0phtCrack의 결과화면을 보여 준다.

특별한 대화들이 시작되여 일부 통과암호들은 이미 해득되였다.

암호화된 NT통과암호들은 \winNT\system32\config등록부안에 SAM이라는 파일이름으로 보관되여 있다. L0phtCrack는 이 정보에 접근하는 3가지 방법을 제공한다.

- 쏘프트웨어가 NT봉사기에서 동작하고 있다면 L0phtCrack안으로 그것을 직접 끌어 들인다.
- 테프, 비상회복디스크 또는 \winNT\repair등록부에 보관된 SAM파일의 여벌판을 읽는다.
- 포함된 readsmb.exe도구프로그람을 리용하여 망전송과정을 감시하면서 SAM파일에 대한 접근을 시도한다.

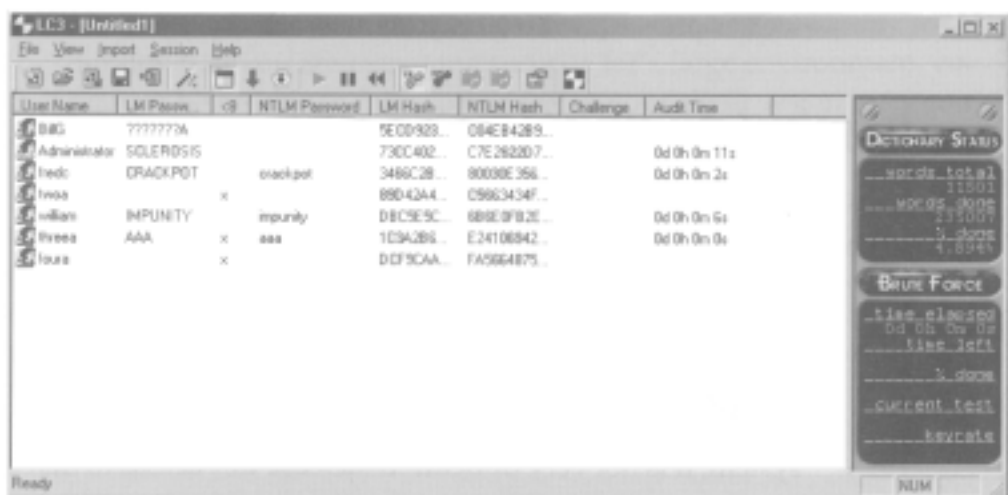



그림 16-12. L0pht의 L0phtCrack 도구프로그람

인증정보들이 일단 수집되면 L0phtCrack도구프로그람에 제공된다. 전체 암호문을 해득하려고 시도하는 일부 통과암호해득기들과는 달리 L0phtCrack는 통과암호를 푸는데 요구되는 시간을 단축하기 위하여 몇개의 간략수법을 리용한다. 실례로 그림 16−12에서 <8렬은 8개문자이하의 통과암호를 가진 구좌를 나타낸다.

이것은 LanMan하쉬에서 암호문을 보고 결정한다. 8개문자이하인 통과암호는 항상 빈자리채우기를 위하여 끝에 문자렬 AAD3B434B51404EE를 첨가한다. L0phtCrack는 이 정보를 리용하여 8개문자이하인 통과암호들을 신속히 결정한다.

통과암호들은 처음에 수천개의 단어를 가진 사전파일에 의하여 검사된다. 사용자가 더 많은 단어들을 추가하려고 한다면 본문편집기로 단어들을 사전파일에 추가할수 있다. 사전파일에 의한 검사는 아주 빠르다. 그림 16−12에서 보여 준 구좌검사는 10s이내에 진행되였다. 사전검색에 의하여 해득되지 않은 통과암호들에 대하여서는 그다음 힘내기공격을 진행한다. 힘내기공격에서는 문자, 수자, 특수문자들을 다 시험할수 있다. 통과암호를 힘내기공격하는데 걸리는 시간은 통과암호의 문자수에 의존한다. 실례로 그림 16−12에서 구좌 cbrenton은 10개문자로 된 통과암호를 가진다. 이 통과암호가 7개문자이하이면 검색시간은 거의 3분의 1로 줄어 든다.

체계관리자는 통과암호해득기의 리용을 마음대로 조종할수는 없다. 일반적으로 통과암호해득기는 매 플래트홈을 위하여서만 리용할수 있다. 그러나 관리자가 봉사기에서 직접 통과암호해득기를 동작시키지 못하도록 차단한다 하여도 공격자는 항상 다른 기계우에서 해득쏘프트웨어를 동작시킬수 있으므로 경계해야 한다.

이것은 진짜 유일한 방어는 통과암호정보를 포함한 모든 파일들을 보호하는것과 함께 경로기와 교환기리용을 통하여 망에 대한 감시를 차단하는것이다.

물리적접근공격

많은 사람들은 망에 대한 공격을 경계할 때 망을 손상시키는 가장 직접적인 방법이 망에 물리적으로 접근하여 진행된다는것은 생각하지 못하고 있다. 격리되거나 또는 페쇄된 지역에서 유지되는 체계는 아주 취약하다. 왜냐하면 체계공격에 필요한 일부 정보들을 가진 공격자라면 체계를 쉽게 손상시킬수 있기때문이다. 이미 강조한바와 같이 공격의 압도적인 대부분은 기관안에서 일어 난다. 기관안에 있는 공격자는 망자원에 대한 일정한 준위의 합법적인 접근권한을 가지고 있다. 체계에 물리적으로 접근할수 있는 공격자가 이 구좌를 관리자준위로 승격시키는것은 그리 어렵지 않다.

실례로 모든 의뢰기체계가 Windows NT Workstation으로 된 망환경을 가정하자. 프로필은 위임배당이며 사용자들에게는 국부체계와 망자원에 대한 최소접근만이 제공된다. 모든 봉사묶음들이 설치되고 보안기능들이 제공된다. 매 NT워크스테이션들은 완전한 검열기능을 리용하여 사건들을 등록하고 의심스러운 동작들을 감시하는 원격프로쎄스로 전송하여 앞으로의 조사를 위한 경과기록정보로 보관한다.

이것은 안전한 의뢰기환경인것처럼 생각되지만 그렇지도 않다. 만일 공격자가 은밀히

기계에 물리적으로 접근한다면 쉽게 다음의 조취들을 취할수 있다.

- 콤퓨터의 씌우개를 벗기고 CMOS통과암호를 지우기 위하여 전원을 방전시킨다.
- 국부파일체계에 대한 접근을 얻기 위하여 플로피디스크없이 체계를 기동한다.
- SAM파일을 복사하고 통과암호해득기를 기동한다.
- 국부관리자통과암호를 제거하여 국부NT조작체계에 대한 완전한 접근을 얻는다.
- 망기판을 련결하지 않고 체계를 재기동하여 어떤 경보에도 걸리지 않고 관리자로 국부가입한다.
- 경과기록준위를 변경하여 의심스러운 동작들이 보고되지 않도록 한다.
- 쏘프트웨어감시기를 설치하여 다른 망통신을 감시할수 있게 한다.
- 다른 망체계를 공격하기 위하여 다른 통과암호를 리용한다.

간단히 말하여 재치 있는 공격자들은 이러한 환경의 보안을 한시간반동안에 완전히 우회한다. 제일 시간이 많이 드는것은 NT의 기동 또는 정지를 기다리는 시간이다. 큰 환경에 대한 보안을 관리할 때 의뢰기체계들을 안전하게 하는 방식으로 보안방책을 세우지 말아야 한다. 우의 설명에서 알수 있는바와 같이 그러한 환경은 너무 쉽게 손상될수 있다.

주 의

례외는 WinFrame 또는 MetaFrame과 같은 약한 의뢰기환경에서이다. 이러한 국부워크스테이션들은 말단보다 약간의 기능을 더 가지고 있다. 즉 모든 보안은 봉사기에 의하여 관리된다.

요 약

이 장에서는 공격자들이 망을 공격하기 위하여 쓰는 일부 방법들에 대하여 설명하였다. 먼저 공격자가 기관이름과 같은 약간의 정보에 기초하여 망에 대한 초기정보를 수집하는 방법을 설명하였다. 다음으로 공격자가 어떤 약점성을 리용하여 공격하겠는가를 알아 내기 위하여 특정한 망환경에서의 조작체계와 봉사류형과 같은 정보들을 어떻게 수집하는가에 대하여서도 설명하였다. 끝으로 공격자가 망자원을 손상시키기 위하여 시도하는 공격방법들에 대하여서도 일부 설명하였다.

다음장에서는 이러한 공격을 어떻게 앞지르겠는가에 대하여 설명한다. 발견된 공격징후들을 어떻게 알려 주며 공격이 시작되기전에 어떻게 망의 약점을 찾아 내는가에 대하여 고찰한다.

제１７장. 공격을 앞지르기

현대 쏘프트웨어가 매우 복잡한것으로 하여 보안취약성은 앞으로 몇년동안 여전히 제기될것이다. 이러한 취약성에 대한 공개적인 토론은 현재 쏘프트웨어에서 악용될수 있는 코드를 제거하는 방향에서 흘러 왔지만 앞으로의 개정판들이 이러한 문제를 완전히 해결한다는 담보는 없다. 실례로 완충기넘침은 1970년대 초부터 프로그람작성자들을 괴롭히고 있지만 오늘도 여전히 많은 문제점들이 제기된다.

안전한 망환경을 유지하기 위하여서는 망관리자가 망환경을 주기적으로 계속 조사하여 약점들이 발견되는 즉시로 대응책을 취함으로써 이러한 약점들이 공격자들에 의하여 악용되지 않도록 하여야 한다. 지난 시기에는 보안문제를 해결하는데서 제품이 갱신되거나 또는 새로운 봉사프로그람묶음이 나오기를 기다려야만 했다. 실례로 Microsoft는 항시적으로 보안과 관련한 기능들을 갱신하여 발표하고 있다. 그러나 제작자들에게서 수정프로그람이 제공되기를 단순히 기다리기만 하여서는 완벽한 보안을 담보할수 없다.

제작자들로부터의 정보

제작자는 최신의 보안림시보수보충프로그람을 얻을수 있는 가장 좋은 통로이다. 대부분 제작자들이 보안상태보고를 제출하지만 일반적으로 특정의 약점에 대하여서는 제3자의 자원을 통하여 훨씬 더빨리 찾을수 있다. 그리고 시장경쟁에 구애되지 않는 정확한 약점정보를 얻는것이 훨씬 더 좋은것이다. 실례로 Microsoft는 뒤구멍(유명한 트로이목마)과 관련한 공개문서에서 다음과 같이 언명하였다.

> 《뒤구멍》은 Windows, Windows NT 또는 Micrsoft Backoffice 묶음제품들에서 실현된 어떤 보안문제도 폭로하거나 악용하지 않는다. 그것은 Windows플래트홈에서 본래부터 존재하는 고유한 보안취약성이 실증될 때까지이다.

이것은 명백히 공개적인 보안관련견해이다. 그러나 이러한 견해는 국부망환경에 위협이 있는가를 결정하려고 하는 체계관리자에게는 큰 도움이 되지 않는다. 이로부터 제작자들이 취약성존재에 대하여 일정한 정도로는 이야기하고 있지만 중요한것은 완전한 최신극비정보를 그어디에선가 구입하는것이다.

3COM

3COM은 망기판과 교환기, 경로기를 비롯하여 많은 종류의 망관련제품을 만들고 있다. 회사는 또한 Palm이라는 손바닥만한 크기의 인기 있는 휴대용콤퓨터들도 제작하고 있다. 3COM은 성능에 비하여 상대적으로 값이 눅은 제품들을 제공한다는데로부터 이름이 만들어 졌다. 3COM의 Web싸이트는 www.3com.com 이다.

기술정보

3COMWeb싸이트는 수많은 기술론문들과 요약들을 제공하고 있다. 목록이 Cisco가 보유하고 있는것만큼 방대하지는 못하지만 3COM싸이트에는 ATM으로부터 망보안측면까지 여러가지 주제의 론문들이 포함되여 있다. 제품에 대한 론문들도 있다. 실례로 방화벽으로서의 3COM NetBuilder리용을 특별히 설명한 보안관련론문들이 있다. 그러나 많은 론문들이 특정한 기술에 대하여 간단히 취급하고 있다.

이러한 론문들은 www.3com.com/technology/tech_net/white_papers /index. html에서 찾을수 있다.

3COM의 Web싸이트에서는 또한 많은 상품지원정보들도 찾을수 있다. 지식과 관련된 정보는 없으나 매 제품에 대한 조언과 관련한 정부와 회사의 설명서 등은 제공한다. 제품과 관련한 문서는 또한 직결봉사를 받을수 있다.

주 의

> 3COM의 지식기지에 대한 접근을 얻기 위하여서는 반드시 계약을 체결하여야 한다. 이것은 이미 알려 진 오유와 같은 더 방대한 범위의 문제들에 접근할수 있는 권한을 준다.

일반적인 지원은 http://infoodeli.3com.com/index.html에서 찾을수 있다.

3COM은 지난 몇년동안 자기의 상품들에 대한 보안상태에서 개선을 가져 왔다. 이것은 그전과는 완전히 대조적이다. 유감스럽게도 3COM은 보안과 관련한 전용우편목록을 가지고 있지 않다. 그러나 다른 제작자들은 제품의 취약성에 대한 통지를 즉시에 할수 있게 전자우편과 같은 봉사들을 제공하고 있다.

수정보충과 갱신

3COM은 모든 자기의 사용자들이 자유로 리용할수 있는 수정보충 및 갱신프로그람을 만들어 제공한다. 봉사계약이 필요없이 그저 받기만 하면 되므로 대단히 편리하다. 즉 봉사계약을 체결함이 없이 오유를 간단히 퇴치할수 있다. 3COM의 지원싸이트에서는 또한 Windows기반 TFTP봉사기와 같은 제3자의 쏘프트웨어도 방조 받을수 있다. TFTP봉사기는 3COM경로기 또는 교환기외의 펌웨어를 갱신하려고 할 때 요구된다. 다음의 쏘프트웨어서고 http://support.3com.com/infodeli/swlib/index.htm 에서 3COM의 수정보충파일들을 얻을수 있다.

Cisco

Cisco는 하부구조의 하드웨어를 전문으로 한다. Cisco는 교환기, 경로기, 방화벽 지어 침입검출체계와 같은 다양한 제품계렬들을 만들고 있다. 인터네트의 대부분은 Cisco하드웨어에서 동작하고 있으며 Cisco는 망련결분야에서 주역을 담당하고 있다. Cisco관련정보는 Web싸이트 www.cisco.com에서 찾을수 있다.

기술정보

Cisco는 망관련정보를 제공하는데서는 인터네트에서 제일 좋은 싸이트이다. 제품서술과 관련한 문서들과 함께 수많은 기술정보들을 제공한다. 특정한 망환경에서 BGP 또는 OSPF를 실행하는데 필요한 정보들까지도 제공한다. Cisco싸이트는 수많은 백서들과 함께 기술적인 설명과 그것을 어떻게 실행하는가를 설명하는 지도서들도 포함하고 있다.

CiscoWeb싸이트는 망관리자들이 자기의 망환경을 엄격히 차단하는데서 도움이 되는 방대한 보안관련문서들도 제공한다. 이 싸이트에서서는 눈물방울공격과 스머프공격에서와 같은 취약성들을 극복하는데 필요한 상세한 정보들을 제공 받을수 있다. 기본페지에 있는 검색엔진으로부터 모든 정보들을 직접 손쉽게 얻을수도 있다.

Cisco는 취약성들을 발견하고 해결하는 우수한 취약성광고기능도 제공한다. Cisco는 CRET를 통하여 이러한 수정보충프로그람들을 발표할뿐아니라 자기자체의 배포통로를 통하여서도 진행한다. Cisco는 취약성이 발견되면 즉시에 수정보충프로그람을 만들어 발표함으로써 인터네트의 주역을 담당한 제작자표준으로 인정되고 있다.

수정보충과 갱신

Cisco는 어떤 부분이 미약하면 새로운 수정보충프로그람을 준비하여 공개하여야 한다. Cisco는 자기의 경로기 또는 교환기들을 수정보충하기 위하여 중요한 문제들은 발표하지 않는다. 오히려 그 회사는 장치의 조작체계를 개선하여 새로운 판번호로 내놓고 있다. 이러한 갱신은 제품의 질제고를 포함하기때문에 Cisco는 공개적으로 접근할수 있는 자기의 Web 또는 FTP싸이트를 통하여 그것들을 쓸수 있게 하지는 않는다. 이러한 갱신프로그람을 받기 위하여서는 Cisco와 계약을 하여야 한다.

Cisco는 주되는 보안구멍이 발견되면 갱신프로그람을 자유로 제공하며 자기의 신용으로 담보한다. 한때 Cisco 700계렬경로기는 매우 긴 통과암호문자렬의 입력과 같은 완충기넘침공격에 취약하다는것이 발견되였다. 이때 Cisco는 봉사계약의 체결여하에 관계 없이 모든 Cisco 700계렬사용자들이 자유로 쓸수 있는 갱신프로그람을 만들어 발표하였다.

Linux

핵심부Linux조작체계는 상업적인 제품은 아니지만 많은 자발적인 지원자들과 그것을 배포하는 각이한 기관들에 의하여 활발하게 제품화되여 제공되고 있다. Linux는 그자체가 특별한 사명을 가진 처리들까지도 조종할수 있는 그러한 견고한 조작체계로서 형성되였다. Linux는 응용봉사기, 경로기, 방화벽으로써도 동작할수 있다. 대부분의 Linux관련정보들은 www.linux.org에 있는 기본Web싸이트에 련결되여 있다.

기술정보

LinuxWeb싸이트는 Linux문서화프로젝트(LDP)에 의하여 만들어 진 방대한 문서들을 봉사한다. 이 싸이트에서서는 자주 제기되는 질문(FAQ)과 사용법(HOWTO), Linux가 제공하는 매 기능들과 봉사들을 그대로 사용하는데 필요한 최소사용법(mini-HOWTO)들과 관련

한 문서들을 제공한다. Linux조작체계를 가지고 무엇을 할수 있는가에 대한 문서는 없다. 오직 Linux의 프로세스 그자체들에 대한 문서들만이 있다. 문서들에는 지어 설치하는 동안 경계할 필요가 있는 많은 경고관련정보들도 포함되여 있다. 문서화에 대한 정보는 www.linux.org/docs/index.html에서 찾을수 있다.

이 페지들에는 또한 많은 Linux관련우편목록과 그룹들에 대한 련결도 포함되여 있다. 이 목록을 이 장에서 그대로 서술하기에는 너무 방대하다. 우편목록을 리용하여 Linux관련문제들에 부닥칠 때 즉시로 방조를 받을수 있다. 전화지원이 필요한 경우에는 료금을 전제로 하여 제작자들이 제공하는 봉사를 리용할수 있다. 제작자의 목록은 www.linux.org/vendors/index.html에서 찾을수 있다.

Linux개발팀은 보안관련취약성들과 수정보충정보들을 발견되는 즉시로 적극적으로 보급하고 있다. 이 정보들은 CRET를 통하여 그리고 많은 Linux토론통로를 통하여 전파된다. Linux개발팀은 또한 보안림시보수프로그람을 발행하는데서 아주 민감하다.

수정보충과 갱신

상업적인 목적을 추구하지 않는 Linux조작체계는 무료로 제공된다. 또한 보안관련 수정보충프로그람들에 대하여서도 마찬가지이다. Linux원천코드를 내리적재할수 있는 일부 URL주소들은 다음과 같다.

- ftp://ftp.cc.gatech.edu/pub/linux/
- ftp://sunsite.unc.edu
- ftp://ftp.caldera.com/pub/
- ftp://ftp.redhat.com/redhat

Microsoft

Microsoft는 자기의 쏘프트웨어제품들에서 발견된 많은 보안취약성들로 하여 지난 몇년동안 심각한 고초를 겪었다. Microsoft는 초기에 보안약점들을 확인하는데서 좀 민감하지 못하였지만 지금은 보조를 맞추고 있다. Microsoft는 현재 어떤 취약성이 보고되면 몇 시간안으로 보안림시보수프로그람을 만들어 발표하고 있다. Microsoft의 Web싸이트는 www.microsoft.com이다.

기술정보

Microsoft의 Web싸이트에는 방대한 기술정보들이 포함되여 있다. 대부분 정보들에는 값비싼 내용이라는 표식이 붙어 있다. 이러한 정보에 접근하는것은 무료이지만 질문항목들에 해당한 내용을 기입할것과 열람기가 cookies를 접수할수 있게 구성할것을 요구한다. 질문항목들은 대체로 누구인가, 어디서 일하는가, 전자우편주소가 얼마인가 하는 항목들이다. 또한 Microsoft로부터 시장정보와 장려하는 내용들을 포함한 전자우편을 앞으로 접수하겠는가를 요구하기도 한다.

이 항목들중에서 열람기가 cookie를 접수하여야 한다는 요구가 가장 큰 문제이다. Cookie는 사용자의 국부체계에 보관되여 있으면서 Web싸이트가 사용자가 누구이며 어디

에 있는가를 식별할수 있게 하는 본문파일이다. Cookie는 Double-Click.net와 같은 회사들에서 기본적으로 리용된다. 그 목적은 지난 시기 사용자에게 제일 흥미를 불러 일으킨것이 어느 광고였는가를 결정하는데 있다. 실지로 놀라운것은 cookie가 사용자의 인터네트 이동상태와 어느 Web싸이트를 방문하여 어떤 문서들을 보았는가를 추적한다는것이다. cookie에 대하여서는 www.netscape.com/newsref/std/cookie-spec.html에서 찾아 볼수 있다.

Cookie를 접수하도록 열람기를 구성할수 없다면 그림 17-1에서 보여 준 오유통보문이 나타날것이다. Microsoft가 이러한 방법으로 사용자에게 자기의 열람기를 리용할것을 요구하기도 한다는것을 고려하여야 한다.

Microsoft는 자기의 Web싸이트로 보안관련통보서를 내보낸다.

수정보충과 갱신

Microsoft는 자기의 Web싸이트를 통하여 모든 보안림시보수프로그람을 자유로 리용할수 있게 한다. Microsoft는 또한 자기의 갱신프로그람들을 갱신통지도구프로그람을 통하여 배포하고 있다. 이러한 도구프로그람들은 Windows체계를 기반으로 동작하며 주기적으로 Microsoft망에 련결되여 현재 어떤 수정보충프로그람이 발표되였는가를 알려 준다. 사용자들은 보안림시보수프로그람들이 발표된 즉시에 내리적재하여 사용할수 있다. 여기서 이미 설명한바와 같이 Microsoft는 보안관련수정보충프로그람을 발표하는데서 아주 민감하다. 이러한 수정보충프로그람들은 FTP싸이트 ftp://ftp .microsoft.com에서 얻을수 있다.

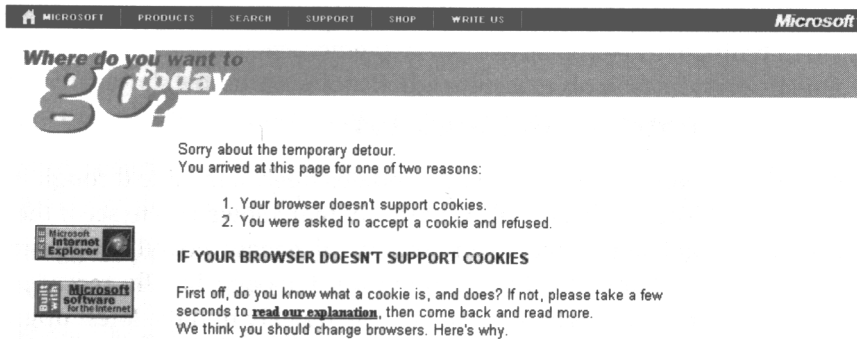



그림 17-1. 기술문서열람에서 쿠키(cookie)의 접수를 요구

Novell

Novell은 NetWare조작체계를 기본으로 여러가지 종류의 망관련제품들을 만들고 있다. Novell은 보안과 관련하여 아주 효과적인 추적레코드를 가지고 있다.

기술정보

Novell의 Web싸이트는 많은 백서들을 포함한다. 그러나 이 모든 문서들은 Novell제품강좌로 특별히 제공된다. 특정한 기술에 대한 일반적인 정보들도 일부 포함되여 있다.

Novell은 자기의 제품강좌들을 위한 직결지도서들을 포함하고 있는 문서싸이트를 제공한다. 문서싸이트의 위치는 www. novell.com/documentation이다.

Novell은 또한 사용자들이 어떤 문제들에 대한 해답을 검색할수 있도록 지식기지를 제공한다. Novell의 기술지원진영에 의하여 조종되는 이 지식기지는 방대하다. 사용자들은 이 지식기지를 통하여 Novell과 관련한 문제들에 대한 해답을 얻을수 있다. 문제는 검색엔진이 사용자들의 요구에 따르는 정확한 문서들을 제공하지 못한다는것이다. 실례로 《Security AND alert》를 입력하면 결과로서 WordPerfect, NetWare Connect, NetView에 대한 제품정보들을 가져 온다. 이 문서들은 취약성과 관련한 정보를 검색하려는 초기질문의 요구에는 맞지 않는다. Novell지원싸이트는 http://support.novell.com에서 찾을수 있다.

주 의

Novell은 CRET상태보고에 관여하지 않으며 자기 싸이트의 일부 공간을 보안관련문제들을 발표하는데 전용으로 리용하지 않는다. 그러나 지식기지에서 보안문제들을 찾을수 있다. 하지만 그것을 찾기 위하여서는 무엇을 먼저 찾아야 하는가를 알아야 한다. 이것은 NetWare제품들에 관하여서는 취약성정보를 전적으로 제3자의 통로에 기초하여 얻어야 한다는것을 의미한다.

수정보충과 갱신

Novell은 자기의 Web싸이트를 통하여 수정보충과 갱신프로그람을 자유로 쓸수 있게 하고 있다. 특정파일에 대한 수정보충이 진행되였는가를 알아 볼수 있도록 파일찾기도구프로그람도 제공한다. 또한 Novell이 제의하는 최소수정보충프로그람을 볼수도 있고 같은 페지에서 내리적재할수도 있다. 최근의 수정보충프로그람들을 한개의 페지에서 찾아 볼수 있으며 가장 최신판을 쉽게 찾아 낼수 있다.

Sun Microsystems

Sun은 UNIX조작체계중에서 가장 인기 있는 계렬들을 제공한다. 이러한 제품들로서는 공학워크스테이션와 고성능응용봉사기들을 들수 있다. Sun은 900MHz의 동작속도를 가진 64bit처리기를 리용한 UltraSPARC제품계렬에서 자기의 성능을 비약적으로 향상시켰다.

기술정보

Sun은 자기의 자원하부구조에서 커다란 개선을 가져 왔다. 대다수의 수정보충프로그람들과 자원정보들은 Sun의 Web싸이트 www.sun.com에서 자유로 찾을수 있다. 이것은 수정보충프로그람들을 별도로 구입하여야 했던 지난 시기와는 완전히 대조적이다.

주 의

Sun은 또한 CRET상태보고에 적극적으로 관여하고 있으며 많은 제작자공보들을 내보내고 있다.

Sun은 또한 Web싸이트의 한개 부분을 배정하여 보안관련정보를 제공하고 있다. 이 페지의 URL주소는 http://sun-solve.sun.com/pub-cgi/show.pl? target= security/sec 이다.

제3의 통로

최신 보안관련약점들을 제공받기 위하여 리용할수 있는 제3자의 자원은 여러가지이다. 이러한 자원들은 망보안을 전문으로 하는 망사용자 또는 그러한 기관들을 방조하기 위하여 형성되였다. 여기에 목록화되여 있는 모든 자원들은 정보접근에서 요구하는것이 하나도 없다는 의미에서 완전히 자유롭게 제공된다. 그러나 자원유지비용을 부담하기 위하여 일부 자원들은 광고로 내보낸다.

제3자의 보안자원에는 취약성자료기지, Web싸이트, 우편목록, 뉴스그룹들이 포함된다. 매개 봉사들은 우점과 결점을 가지고 있다.

취약성자료기지 약점들을 찾기 위한 검색기능은 제공하지만 검색결과를 다시 추가질문으로 할수 있는 귀환기능이 없다.

Web싸이트 수정보충프로그람에 대한 직접련결뿐아니라 상세한 설명도 제공하지만 특정의 약점을 찾는데 많은 품이 든다.

우편목록 찾으려는 약점에 대하여 즉시에 통보를 제공하지만 일부 목록들은 매일 50개이상의 통보문들을 보관할수 없는것도 있다.

뉴스그룹 특정한 약점에 대하여 더 상세한 내용을 제공하지만 요구하는 정보를 찾기 위하여 많은 통보문들을 엄밀히 조사하여야 한다는 복잡성이 있다.

일러두기

약점들을 정상적으로 통보 받기 위하여서는 하나 또는 두개의 우편목록들에 기입하여 의뢰하는것이 제일 좋다. 그다음 특정한 문제들을 구체적으로 조사하기 위하여 취약성자료기지와 Web싸이트를 리용할수 있다.

취약성자료기지

취약성자료기지는 특정한 기준에 기초하여 약점들을 검색할 때 리용한다. 실례로 특정한 조작체계(NT,Linux 등)에 영향을 미치는 약점들을 특정공격류형(봉사거부, 해득)에 맞게 검색할수 있다. 지어 특정한 날자들에서만 발견되는 약점들도 검색할수 있다.

IIS의 X-Force 자료기지

인터네트보안체계(ISS)의 X-Force자료기지는 플래트홈 또는 실마리어에 의하여 검색할수 있다. 사용자들의 취미에 따라서 UNIX는 7개의 부류로, 모든 Windows조작체계는 하나의 부류로 그룹화하였다. 자료기지는 조작체계약점들만 목록화하였다. 즉 3COM 또는 Cisco장치와 같은 망관련하드웨어에 대하여서는 목록화하지 않았다. 특정한 플래트홈에 대한 모든 내용 또는 매달에 가치 있는 보안관련약점들만 선택하여 참고할수 있다. 또한 선택된 내용들을 한페지에 요약하여 또는 전부 현시되게 할수도 있다.

X-Force자료기지의 고유한 특징은 매 항목들에 위험준위를 할당한것이다. 만일 문의

결과가 여러개의 항목들로 주어 진 경우 목록을 조사하여 제일 나쁜 항목들을 신속히 찾아 낼수 있다. 자료기지의 매 항목들은 비록 100%의 정확도를 담보하지는 않지만 내용들을 충분히 서술하고 있다. 실례로 앞장에서 설명한 Exchange약점을 찾으면 결과는 다음과 같다.

> 이 공격은 Exchange봉사기의 기동정지를 일으킨다. 이 공격에 의하여 Exchange봉사기에서 유지되는 자료의 분실 또는 그것에 대한 불법접근이 일어 나지는 않는다. Exchange봉사기는 또한 공격자가 주소부분에 코드를 삽입하고 그것을 실행시킴으로써 일어 나는 탄창겹쳐쓰기공격에 약하다.

여기서 알수 있는바와 같이 이 항목에는 일부 모순점들이 있다. 공격이 봉사기의 기동정지를 일으킨다면 그 순간에 주기억에만 보존되여 있고 디스크에는 아직 보관하지 못한 자료들은 분실된다. 또한 불법접근이 일어 나지 않는다는 첫번째 내용은 그다음의 코드를 삽입하고 그것을 실행시킬수 있다는 내용에 모순된다.

X-Force자료기지는 http://xforce.iss.net에서 찾을수 있다.

Packet Storm

Packet Storm은 《세계에서 제일 크고 최근에 갱신된 정보보안관련자료》로 발표하고 있다. 실제로 Packet Storm은 정보보안의 모든 측면에서 가장 포괄적인 검색과 보고기능을 제공하고 있으며 주어 진 체계의 약점뿐만아니라 정보보안분야에서 최근에 일어 나고 있는 모든 상태를 구체적으로 통보하는 새로운 봉사도 제공하고 있다.

Packet Storm은 자료기지에서 자주 반복되여 검색되는 주제들을 보고하도록 Storm Watch라는 고유한 특성도 제공한다. 20번이상의 검색이 요구된 질문들을 표 17-1에 제시하였다.

표 17-1　　자주 반복되는 보안질문

질 문	날 자
apache	Sun Feb 18 10:52:22 PST 2001
named	Sun Feb 18 10:52:20 PST 2001
firewall software windows	Sun Feb 18 10:52:18 PST 2001
linux 2.0.35	Sun Feb 18 10:52:18 PST 2001
ssi exec	Sun Feb 18 10:52:15 PST 2001
pimp.c	Sun Feb 18 10:52:13 PST 2001
unix keylogger	Sun Feb 18 10:52:05 PST 2001
epmap	Sun Feb 18 10:52:04 PST 2001
proftpd 1.2.0pre2	Sun Feb 18 10:52:03 PST 2001
exec cmd	Sun Feb 18 10:52:01 PST 2001
NT 4.0	Sun Feb 18 10:51:49 PST 2001

표계속

질 문	날 자
apache exploit	Sun Feb 18 10:51:48 PST 2001
rootshell	Sun Feb 18 10:51:28 PST 2001
mail	Sun Feb 18 10:51:25 PST 2001
uin sniffer	Sun Feb 18 10:51:24 PST 2001
windows 98	Sun Feb 18 10:51:23 PST 2001
php	Sun Feb 18 10:51:12 PST 2001
+apache+exploit	Sun Feb 18 10:51:10 PST 2001
solaris	Sun Feb 18 10:51:08 PST 2001
windows 98	Sun Feb 18 10:51:08 PST 2001

Packet Storm은 http://packetstorm.security.com/에서 찾을수 있다.

보안결점 (Security Bugware)

실제의 자료기지보다 더많이 목록화되여 있는 보안결점취약성자료기지싸이트에는 인터네트의 모든 싸이트들에 대한 약점들과 취약성들을 포괄하여 완전히 목록화되여 있다. 이 방대한 정보에 아마 깜짝 놀랄것이다. Windows에 대한것만 하여도 250개이상의 항목들이 포함된다. 그가운데서 일부는 좀 반복된다. 실례로 Ping에 대하여 5개의 항목으로 설명하고 있으며 그중 3개는 죽음의 Ping에서 다시 반복된다. 그러나 이러한 반복은 실제로 아주 편리하다. 왜냐하면 취약성들이 어떻게 악용될수 있는가 하는 더 구체적인 표상을 줄수 있기때문이다.

항목들에 대한 검색기능은 없다. 12개의 조작체계부류에서 하나를 선택하고 결과를 통하여 검색을 시작한다. 항목들은 자모순서대로 목록화되여 있으므로 검색은 그리 어렵지 않다. 또한 Web열람기의 Find기능을 리용하여 일부 검색기능을 대신할수 있다.

주 의

취약성목록은 목록화된 제품의 다양성에 관하여서도 또한 완성되였다. 조작체계의 기본목록뿐아니라 망관련하드웨어와 망응용프로그람에 대한 취약성항목들도 찾을수 있다. 만일 하나의 취약성자료기지에 련결되여 있다면 그것에 대한 항목들만을 찾을 수 있다.

이 싸이트는 http://161.53.42.3/~crv/security/bugs/list.html에서 찾을수 있다.

Web싸이트

제3자의 Web싸이트들에는 모든 형태의 보안관련발표에 대한 수많은 정보들이 포함되여 있다.이 싸이트들에서는 망환경을 보안하기 위한 지침들과 함께 공격자들이 다른 망을 공격할 때 리용하는 도구들까지도 제공한다. 많은 보안관련싸이트들에서 몇개를 선택하여 설명하기로 하자.

AntiOnline

AntiOnline은 모든 관련내용들을 요점적으로 제공하는 싸이트들중의 하나이다. 기본페지에는 망보안과 관련한 현재 새 소식들의 목록이 있다. 또한 《Quick Tips》단락으로 속임주소추적과 같이 망관리자에게 필요한 매일매일의 보안문제들 또는 대량살포되는 광고성전자우편에 대하여 아주 적중한 조언들을 제공하고 있다. 또 다른 련결을 통하여 방대한 범위의 보안주제들에 대한 론문들을 보존하고 있는 직결도서관들을 열람할수 있다. 또한 기능상 서로 반대되는 수많은 보안도구들을 포함하고 있는 보존파일도 제공한다. AntiOnline은 www.antionline.com/에서 찾을수 있다.

CERT홈페지

콤퓨터긴급응답기구(CERT)은 인터네트기반에 있는 약점들을 수집할 사명을 지닌 싸이트를 운영하고 있으며 취약성을 해결하는 다른 제작자들과도 협력하고 있다. CERT는 또한 알려 진 취약성들에 대하여 공개적인 통보를 발표하고 있다.

주 의

CERT는 UNIX취약성에 선차적인 관심을 돌리지만 Windows취약성에 대하여서도 발표하고 있다.

싸이트는 또한 망환경을 보안하는데서 도움이 되는 지도서들도 제공한다. CERT는 www.cert.org/ 에서 찾을수 있다.

손해를 주지 않는 해킹지도서

이름과는 달리 공격에 대처하는데서 대단히 유용한(비록 좀 뒤떨어 졌지만) 싸이트이다. 어떻게 공격을 전개하며 어떻게 그것을 차단하는가 하는 많은 실례들이 제공된다. 모든 실례들은 독자들이 약간의 콤퓨터실천경험을 가지고 있는것을 전제로 하여 지도서들을 리해하기 쉽게 편성하였다. 안내서는 www.spaziopiu.it/elettrici/gtmhh/에서 찾을수 있다.

L0pht와 @stake

L0pht는 보스톤지역에서 체계보안과 암호화를 전문으로 하는 해커들의 집단으로부터 시작되였다. 이 싸이트들은 상태보고와 도구들을 포함하여 수많은 보안관련정보들을 제공한다. 잘 알려 진 일부 취약성들은 L0pht의 검사서고에서 찾을수 있다. 이것은 L0pht의 대부분 상태보고들이 직접 체험하여 얻은 정보에 기초하고 있다는것을 의미한다.

2000년 1월에 L0pht는 새로 형성된 회사인 @stake(compaq, Forrester Research, Cambridge Technology Partners의 이전 직원들에 의하여 만들어 졌다.)와 련합하였다. L0pht의 이전 성원들이 지금 @stake에서 연구서고를 운영하고 있기때문에 Web싸이트는 보안상태보고에 대한 가장 좋은 자원들을 계속 유지하고 있다. L0phtcrak와 Antisniff와 같은 L0pht에 의하여 개발된 많은 도구들이 지금 보안쏘프트웨어기술에 의하여 배포되고 있으며 이 도구들은 www.securitysoftwaretech.com에서 찾을수 있다. 연구서고에 의하여 개발된 더 새로운 도구들은 여전히 국부Web싸이트의 기본봉사로 제공되고 있다. 연구서고는 www.atstake.com/research/index.html 에서 찾을수 있다.

국가보안협회

국가보안협회(NSI)홈페지는 망의 범위를 초과하여 다양한 주제에 대한 보안관련정보들을 제공한다. 콤퓨터보안과 함께 싸이트는 개인보안, 테로, 보안법령 지어 려행상태보고와 같은 정보들도 제공한다. 싸이트의 정보는 매우 다양하다. 심지어 정보보안방책에 대한 심리적효과론문들도 읽을수 있다. 이 싸이트는 보안분야의 지식을 폭넓게 소유하는데 필요한 모든 자원들을 제공하는 아주 편리한 싸이트이다. NSI홈페지는 http://nsi.org/에서 찾을수 있다.

Phrack 잡지홈페지

Phrack잡지는 체계취약성과 관련하여 가장 오래동안 운영되고 있는 전자공학잡지이다. 상당히 많은 약점들이 Phrack홈페지로부터 공개되여 알려 졌다. 대다수의 기사들은 어떻게 약점을 악용하는가 하는 관점에서 설명하지만 일부 기사들은 파괴적인 공격의 후과에 대하여서도 상세히 서술하고 있다. 이것은 공격을 막아 낼수 없는 경우 어떤 자원을 보호하여야 하는가를 확인하기 위해서도 꼭 필요한 정보이다. Phrack는 어떠한 예정표도 내놓지 않는다. 제일 최근의 문제점 #56은 2000년 5월에 발표하였다. Phrack는 자기의 Web싸이트를 가지고 있지 않지만 제공하는 정보들은 http://packetstorm.security. com/mag /phrack/ 에서 찾을수 있다.

Robert Malmgren의 NT Security FAQ

이름이 표현하는바와 같이 이 싸이트는 NT관련내용(Windows 2000정보는 아니다.)들을 제공한다. 이 싸이트는 NT봉사기의 보안과 관련하여 알고 싶은 모든 정보들을 제공한다. 관리와 등록고, 파일체계를 포함하여 NT봉사기의 모든 측면들을 매우 상세히 설명한다. 또한 NT와 호환성이 있는 방화벽과 인증에 대한 정보를 제공하는 내용도 포함되여 있다. NT봉사기를 보안할 필요가 있으면 이 싸이트에서 가치 있는 정보들을 참고할수 있다. NT Security FAQ는 www.it.kth.se/~rom/ntsec.html에서 찾을수 있다.

우편목록

우편목록은 보안취약성을 정상적으로 통보할수 있는 아주 쓸모 있는 도구이다. 우편목록은 취약성이 공개적으로 발표되면 즉시에 해당한 통보를 제공한다. 또한 특정의 약점들에 대하여 구체적으로 론의할수 있는 공개토론회를 지원하는 가능도 제공한다. 우편목록들은 서로 련결되여 정보를 제공하기때문에 특정한 약점들에 대하여서는 취약성자료기지보다 더 많은 정보를 제공한다. 열린 공개토론회에서는 자유롭게 질문할수 있다.

주 의

우편목록에 등록하기 위하여서는 우편목록봉사기에 전자우편통보문을 보내야 한다. 이 통보문은 본체부에 subscribe와 같은 열쇠단어 또는 단어형태를 포함하여야 한다. 목록에서 제거하려면 unsubscribe단어를 리용하여 우의 처리과정을 반복하면 된다.

Bugtraq

모든 취약성토론목록의 모체인 Bugtraq는 약점에 대한 토론을 조정하는 우편목록이다. 많은 취약성들이 이 목록에 의하여 처음으로 발표되였다. 우편목록은 어떤 약점들이 발견되였으며 그것을 수정하기 위하여서는 무엇을 하여야 하는가에 기본을 둔다. 발견된 어떤 취약성에 대하여 통보 받았다는것을 보증하기 위하여 서명하는 목록도 있다. 자료흐름이 좀 많지만 이 목록을 통하여 매일 여가시간에 몇번의 마우스찰칵으로 수집되는 정보는 아주 가치 있는것이다. Security Focus는 Bugtraq의 보존과 서명형식에서 기본기능을 담당한다. Security Focus는 www.security.com/about/feedback/subscribe.html 에서 찾을수 있다.

Firewall-Wizards

방화벽조수우편목록(Firewall-Wizards mailing list)은 방화벽과 주변보안과 관련된 모든 주제들을 토론하는 우편목록이다. 이 목록은 모든 우편들이 주제에 맞게 정상적으로 동작하는가 그리고 모든 광고성전자우편들이 려과되는가를 확인하고 있는 Macrus Ranum에 의하여 조정된다. 자료흐름준위는 방화벽연구로 인한 일부 과도한 경우를 제외하고는 극히 낮은 경향성을 가진다. 목록에는 방화벽과 관련한 요점들을 선택하는데서 큰 역할을 담당수행하는 아주 우수한 일부 성원들만이 포함되여 있다.

더 상세한 정보와 목록가입과 관련한 정보들은 www.nft.com/mailman /listinfo/firewall-wizards에서 찾을수 있다.

InfoSec News

InfoSec News우편목록은 보안관련 새소식들을 보급한다. 여기에는 신문, 잡지, 직결참고서에서 일하는 전문가들이 포함되여 있다. 우편목록은 닫겨 져 있다. 즉 조정자에 의하여서만 보급이 진행된다. 다른 성원들은 조정자에게 보안관련 새소식들을 보내는것으로써 정보봉사에 기여한다. 목록은 보안분야에서 화제로 되고 있는 많은 취약성들에 대하여 그 일부만을 론의하고 있다. 목록가입과 관련한 상세한 정보는 www.c4i.org/isn.html에서 찾을수 있다.

IIS의 X-Force IDS 토론목록

IIS는 자기의 Web싸이트를 운영하고 X-Force에 있는 많은 토론목록들에 대한 중계자적역할을 담당수행하고 있다. 이 싸이트에서는 제일 인기 있는 분야의 하나인 침입검출체계우편목록을 운영하고 있다. 이 목록은 침입검출체계와 관련한 주제들에 중점을 두고 있으며 특정한 사람에 의하여 운영이 조정되지는 않는다. 이 목록은 열린 공개토론회형식으로 운영된다. 즉 모든 사람들은 자유로 질문 또는 그것에 대한 대답을 배포할수 있다. 목록에 가입하기 위하여서는 열람기에서 http://xforce.iis.net/maillists/를 열람하면 된다.

NT Bugtraq 우편목록

NT Bugtraq우편목록은 다만 MicrosoftWindows의 취약성과 그로부터 초래되는 공격들을 기본초점으로 하여 운영된다. 이름과는 달리 Microsoft조작체계와 응용프로그람에 대한 문제도 토론된다. 목록은 발송을 될수록 최소화하는 방책에서 매우 힘들게 조정된다. 사실 대부분은 목록조정자 또는 Microsoft프로그람작성자들로부터 발송된다. Windows에 커다란 흥미를 가지고 있다면 이 목록에 가입하여 많은 정보를 교환할수 있다.

주 의

Bugtraq우편목록에서 토론되는 Windows와 관련한 취약성들을 이 목록에서도 찾을수 있다.

NT Bugtraq에 대한 더 구체적인 정보와 목록가입에 대하여서는 www.hntbugtraq. com에서 찾을수 있다.

뉴스그룹

보안관련주제들을 취급하는 많은 그룹들이 있다. 뉴스그룹들은 아무런 절차없이 가입할수 있는 매우 편리한 정보공유기능을 제공한다. 통보문은 뉴스그룹봉사기로 발송되며 여가시간에 그것을 읽어 볼수 있다. 뉴스그룹에서 한가지 문제는 그것이 대단히 높은 신호 대 잡음비를 가진다는것이다. 이것은 뉴스그룹공개토론회가 그 누구에 의하여 조정되는것이 아니기때문이다.

주 의

높은 신호 대 잡음비란 많은 발송우편들을 려과하여야 실지로 흥미를 가지는 정보를 찾게 된다는것을 의미한다.

여기에 흥미 있는 일부 뉴스그룹들을 목록화하였는데 설명은 하지 않았다. 왜냐하면 뉴스그룹이름들이 다 자기의 기본주제를 반영하고 있기때문이다.

- comp. os.ms-windows. nt. admin. security
- comp. os. NetWare. security
- comp. security. firewalls
- comp. security. ssh
- comp. security. unix
- comp. security. misc
- microsoft. Public. Access. security

환 경 검 열

여러개의 봉사기들을 가진 망환경을 보안하는것은 아름찬 과제이다. 혼자서 체계를 어떻게 방어하겠는가를 생각하고 매일 점검을 하는것은 매우 어려운 일이다. 특히 많은 부하가 걸려 있는 망관리자는 다른 여가시간을 얻기 위하여 보안문제를 뒤로 미루어 놓을수 있다.

문제는 매번 무엇을 찾아야 하는가를 모르는데 있다. 대부분의 망관리자들은 설정을 변경하거나 또는 요구되는대로 수정보충프로그람을 적재한다. 그러나 기본은 보안을 위하여 무엇이 필요한가에 대한 어떤 방향을 가지고 있어야 한다. 제일 명백한 선택은 보안상담자를 채용하는것이다. 물론 이것은 예산안에 포함되여 있어야 한다.

약점들을 수정하려고 한다면 제16장에서 설명한 취약성스캐너를 리용하여 시작하는것이 제일 합리적이다. 인터네트보안체계(ISS)와 WebTrends에서 제공되는 제품들은 약점들을 문서화하는데서 아주 편리하다. 그러나 때때로 어떤 방향에서 계산환경을 더 안전하게 할수 있겠는가 하는 문제도 제기된다. 이러한 경우에는 보안검열프로그람을 리용하여야 한다.

보안검열프로그람묶음은 오유 또는 알려 진 취약성들을 찾아 내지는 못한다. 그보다는 망상의 모든 체계들이 설정한 보안방책에 따르는가를 확인한다. 실례로 보안방책이 모든 사용자구좌들이 90일만에 통과암호를 반드시 변경하도록 설정되였다면 검열프로그람묶음은 봉사기의 매 사용자들을 검사하여 변경사항을 검열한다.

Kane보안분석기

침입검출(Intrusion Detection)의 Kane보안분석기(KSA)는 봉사기검열프로그람묶음이다. 취약성검사는 진행할수 없지만 매 봉사기들에 대하여 보안방책추종준위를 평가한다. KSA는 Windows NT와 NetWare(bindery, NDS), UNIX 지어 Lotus Notes봉사기들도 검열할수 있다.

KSA는 사용자구좌와 파일체계, 경과기록 지어 NT/2000체계의 등록고까지도 검사한다. 기관의 보안방책의기준을 입력하면 KSA는 어느 망봉사기가 이에 추종하지 않는가를 보고한다.

실례로 Windows 2000을 사용할 때 KSA의 검열기능을 리용하여 보안방책을 검열할수 있다.

주 의

Windows NT/2000에 대한 검열처리와 보고는 다른 플래트홈들에서도 거의 류사하다. 차이는 KSA가 등록고허가를 검열할수 있으며 어느 구동기가 NTFS를 리용하고 있는가를 확인한다는것이다.

KSA의 30일평가판본은 www.intrusion.com에서 내리적재할수 있다.

KSA의 설치

KSA의 설치는 단순하지 않다. KSA의 Web싸이트에서 최신판을 내리적재하고 자동추출실행방식으로 이행(림시등록부로 이행)한 다음 setup.exe파일을 실행한다.

설치프로그람은 설치할 등록부위치를 요구한 다음 요구되는 모든 파일들을 설치한다. KSA의 제거는 조종판의 추가/제거프로그람그림기호를 조작하여 진행할수 있다.

주 의

KSA는 Windows NT Server/Workstation 3.51판이상에서 동작시켜야 한다. Wiundows 95/98에서는 성과적으로 설치되였다고 하여도 동작은 하지 않는다.

KSA는 NT/2000체계에 설치하고 봉사기들을 원격에서 검열할수도 있다. 이때 매 체계에 KSA를 설치할 필요는 없다. 설치가 끝나면 Kane보안분석기프로그람으로 가서 Kane보안분석기그림기호를 찰칵한다.

KSA의 리용

KSA의 기본화면을 그림 17-2에 보여 준다. 추종검열은 3단계로 진행된다.

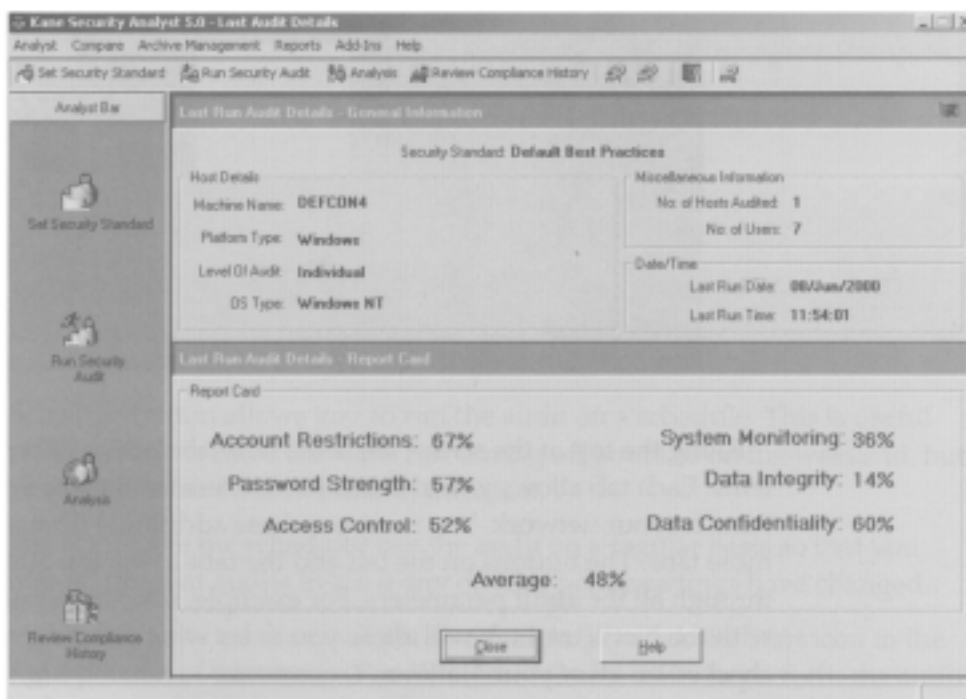



그림 17-2. KSA의 기본화면

1. 보안표준을 설정한다.
2. 보안검열을 실행한다.
3. 보안검열의 분석결과를 현시한다.

매 단계들은 화면의 아래로 내려 가면서 순차적으로 다른 단추들로 표현되여 있다. 네번째 단추는 추종리력을 조사하는데 리용된다. 일단 검열이 끝났다면 화면우에 있는 그림기호를 리용하여 검열결과를 부분적으로 볼수 있도록 선택한다.

보안방책정의

보안방책은 보안표준설정단추를 눌러서 현시되는 화면(그림 17-3)에서 입력한다. 화면의 왼쪽에 있는 단추들을 리용하여 보안방책을 여러가지 측면에서 선택할수 있다. 실례로 기정으로는 구좌제한이 선택된다. 이 단추에서는 KSA가 콤퓨터와 시간제한을 리용하여 검사하겠는가를 정의할수 있게 한다. 또한 KSA가 무효구좌 또는 휴식상태에 있는 구좌도 검사하는가를 정의한다.

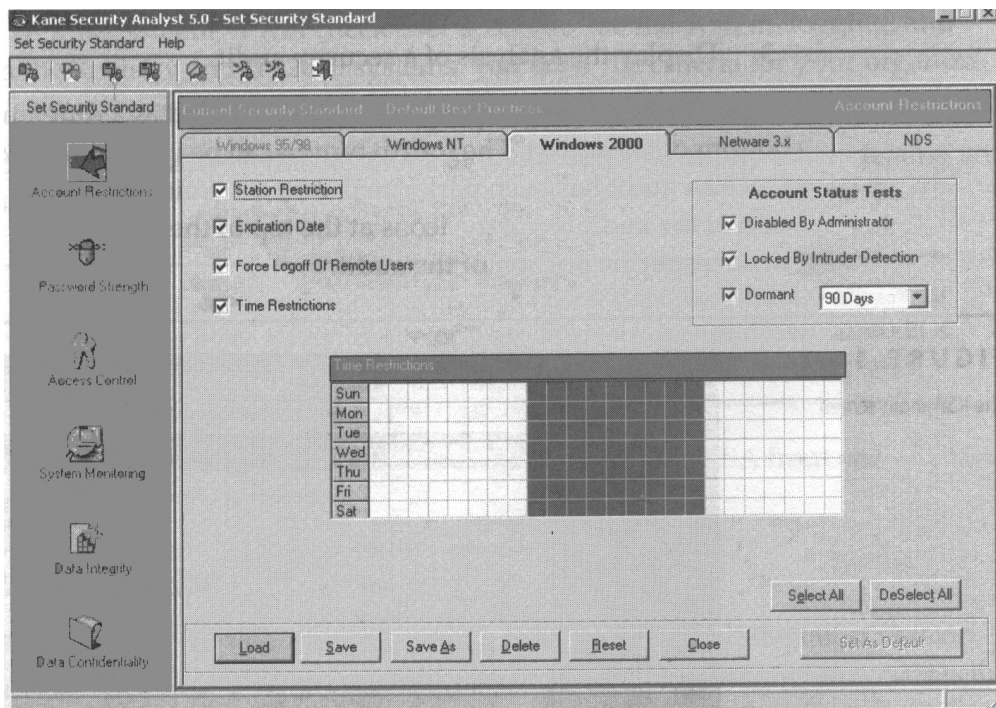



그림 17-3.구좌제한에 의한 보안방책설정

화면의 우에서 각이한 조작체계를 표현하는 표적들이 있다. 여기서는 망체계에서 사용할수 있는 조작체계들을 선택할수 있다. 이 표적들을 선택가능하게 하기 위하여서는 사용권을 추가로 구입하여야 한다. 화면의 왼쪽에 있는 단추들과 우에 있는 표

적들을 리용하여 모든 검열파라메터들을 설정할수 있다. 실례로 NetWare4라는 표적파체계감시단추를 선택하여 모든 NetWare 4.x봉사기들에서 경과기록을 검사하도록 설정할수 있다.

검열실행

검열실행은 KSA기본화면에서 보안검열실행단추를 선택하여 진행한다. 보안검열실행창을 그림 17-4에 보여 준다. 여기서는 KSA가 선행한 검열을 다시 갱신하여 진행하는가 또는 령에서 새로 시작하는가를 확인할수 있다. 또한 검열시에 검사하려는 체계 또는 령역을 선택할수 있다.

일정계획단추는 검열을 계획화하여 수행할수 있게 한다. 만일 주말에 또는 제정된 시간에 검열실행을 하려는 경우 편리하다.

일정계획단추는 검열을 규칙적으로 진행하고 다른 검열들과 비교함으로써 보안방책설정이 변경되였는가를 확인하는데 리용할수 있다.

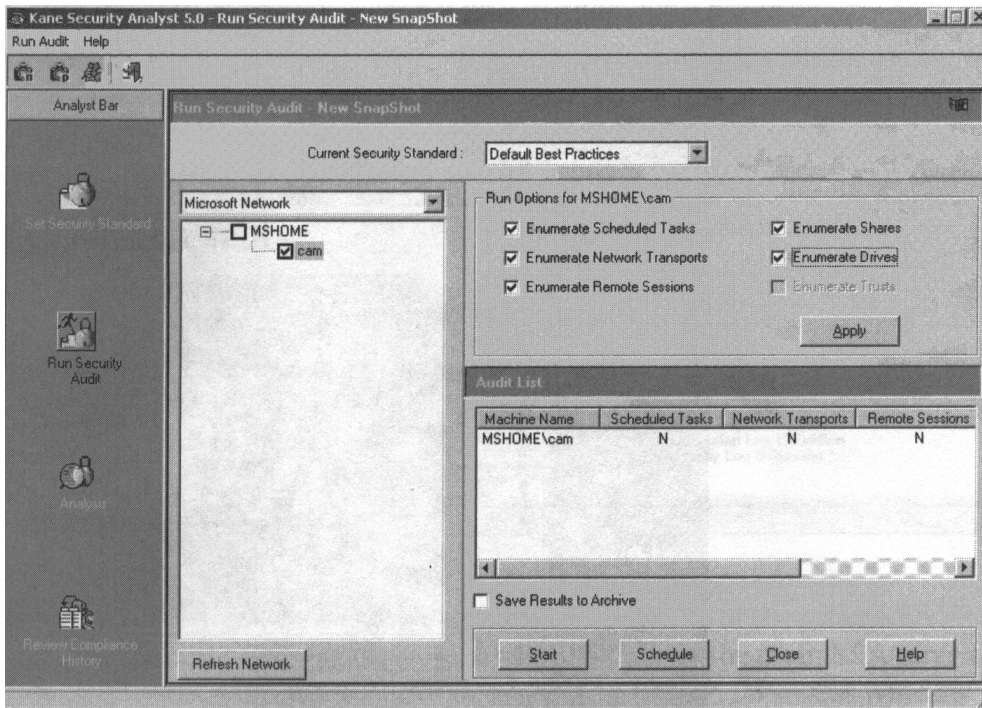



그림 17-4. 보안검열실행창문

일단 검열파라메터들을 선택한 다음 화면의 아래부분에 있는 시작단추를 누르기하여 실행을 개시한다. 검열실행시간은 검열을 진행하는 기계의 속도와 KSA가 검열하는 체계들의 수에 관계된다. 검열이 완성되면 결과를 조사한다.

검열결과의 조사

검열결과는 KSA기본화면에서 위험분석조사단추를 선택하여 그라프적인 개괄로서 조사된다. 그림 17-5에 위험분석조사화면을 보여 주었다. 그라프들은 체계구성의 어느 부분이 보안방책지침에 맞고 어느 부분이 맞지 않는가를 보여 준다. 100%가 완전한 추종을 나타낸다. 낮은 부분들은 체계에 어떤 조종이 필요하다는것을 나타낸다. 추종프로그람은 망관리자가 먼저 주의를 돌려야 하는 부분이 어디인가를 결정하는 척도로서 리용할수 있다.

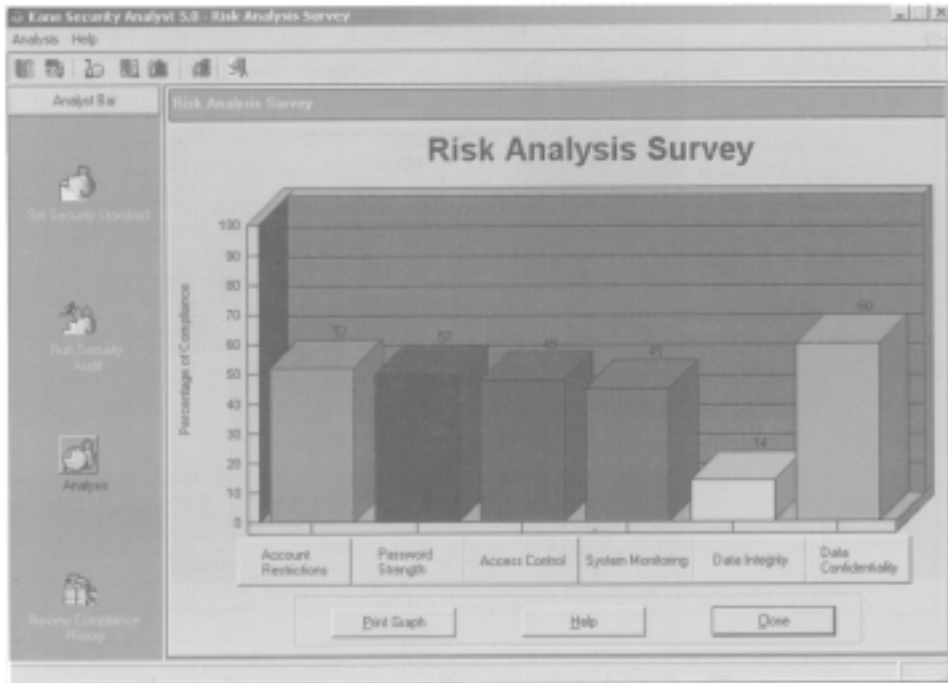



그림 17-5. 위험분석조사화면

위험분석조사창에서 체계감시단추를 선택하여 체계의 보안상태가 미약한 원인에 대한 구체적인 정보를 얻을수 있다. 그림 17-6에 체계감시화면을 보여 준다. DEFCON4는 체계감시결과 보안상태가 매우 미약한것으로 평가되였다. 원인은 사건경과기록과 유지시간이 정확히 구성되지 못했기때문이다. 모든 봉사기프로그람들이 이 특징을 리용하도록 보안방책이 설정되여 있으므로 KSA는 이 체계에 대한 검열을 단념하였다. 화면의 오른쪽 아래창에 있는 Security Log Size는 경과기록공간이 너무 작아서 기록입구점들을 충분한 기간 보존할수 없다는것을 나타낸다.

이 정보는 아주 쓸모가 있다. 왜냐하면 이 체계를 보안방책에 정확히 추종하도록 하기 위하여서는 어떤 설정항목들을 수정하여야 하는가를 체계관리자가 정확히 알수 있게 하기때문이다.

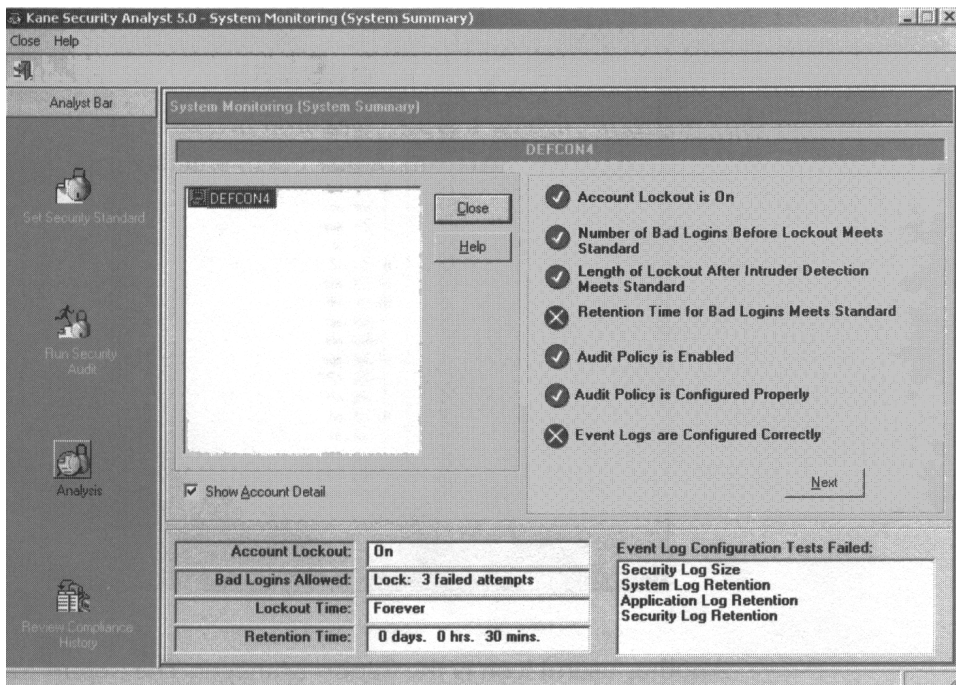



그림 17-6. 체계감시화면

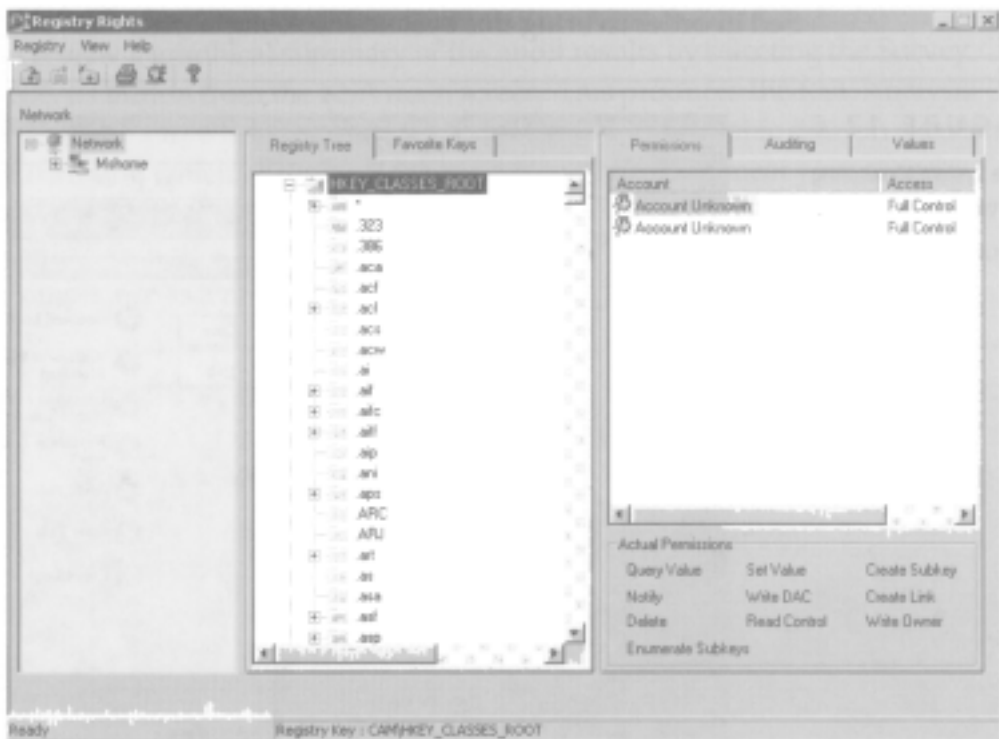



그림 17-7. 등록고권한화면

KSA는 이밖에 다른 특징들도 가지고 있다. 실례로 KSA기본화면에서 등록고권한그림기호를 찰칵하면 그림 17-7에 보여 준 등록고권한화면이 나타난다. 이 화면에서 매 사용자 또는 그룹에 할당된 접근권한을 조사할수 있다. 왼쪽판에서는 등록고를 항목별로 조사할수 있으며 오른쪽판에서는 누구에게 접근이 할당되였으며 어떤 준위의 허가가 보증되는가를 조사할수 있다. 추가단추는 이 등록고열쇠를 특별히 따로 취급할수 있게 한다.

허가를 검사하기 위하여 등록고의 전체 나무를 조사하는것은 많은 시간을 랑비한다. 실제로 규칙적인 점검에서는 SAM열쇠와 같은 등록고열쇠들만을 검열한다. Favority keys 표적은 망관리자가 기본으로 검사하려는 열쇠가 어느것인가를 지적할수 있게 한다. 기본열쇠들을 지적한 다음 Favorit keys표적을 선택하여 기본열쇠들을 하나의 구역에서 볼수 있다. 이러한 기능은 허가설정을 검사할 때마다 매번 등록고를 검색하여야 하는 부담을 덜어 준다.

또 다른 유용한 기능은 보고관리기능이다. 이 기능은 보고서에 어떤 정보가 반영되는가를 선택하도록 함으로써 검열처리를 간단히 할수 있게 한다. 실례로 매 봉사기에서 동작하는 모든 봉사들과 오유기록입구점들만을 포함하는 하나의 보고서를 만들수 있다. 이것은 모든 망봉사의 정상상태를 신속히 확인할수 있게 한다.

결과대책

검열이 끝난 다음에는 검열결과에 기초하여 대책을 취하여야 한다. KSA는 보안에 대한 정확한 의견을 주기때문에 아주 우수한 도구이다. 체계는 입력한 보안방책에 기초하여 확인된다. 이것은 체계가 임의로 정한 일부 표준들에 기초하여 검사되지 않는다는것을 의미한다. KSA에서는 체계가 이미 결정하여 구성한 보안방책에 추종하는가 안하는가를 검사한다. 그러므로 KSA는 임의의 망환경에 적응할수 있게 모형화할수도 있다.

요 약

이 장에서는 발견되는 약점들을 정상적으로 알고 있으려면 어떻게 하여야 하는가를 고찰하였다. 또한 취약성을 찾기 위하여 어떤 제작자와 제3자의 자원을 리용할수 있는가 그리고 어디에서 보안림시보수프로그람들을 얻을수 있으며 더 많은 정보를 얻기 위하여서는 우편목록과 뉴스그룹들을 리용한다는데 대하여 설명하였다. 끝으로 망환경에 대한 보안검열을 어떻게 진행하는가 그리고 이것을 지원하는 도구들에 대하여 설명하였다.

부록 1. CD-ROM에 대하여

CD-ROM에는 망의 취약성을 식별하고 고의적인 공격으로부터 망을 보안하는데 리용할수 있는 보안쏘프트웨어제품들이 포함되여 있다. Sybex는 쏘프트웨어회사들과의 협력을 통하여 이 제품들을 사용자들에게 제공한다. 설치와 관련한 정보들을 아래에서 설명한다. 더 자세한 정보에 대하여서는 readme파일을 참고하시오.

주 의

이 제품들을 설치하기 위하여서는 Windows NT 4.0이 필요하다.

방화벽-1(FireWall-1)

CD에는 Check Point 쏘프트웨어기술회사에 의하여 30일평가판본으로 제공되는 FireWall-1이 포함되여 있다. FireWall-1은 다음의 조작체계들에서 동작시킬수 있다.

- Windows NT 4
- Windows 2000
- Red Hat Linux 6.1
- Sun Solaris 2.6, 7
- HP-UX 10.20, 11.0
- AIX 4.2.1, 4.3.2, 4.3.3

주 의

보안리유로 하여 Check Point로부터 인증열쇠를 받기전까지는 FireWall-1의 완전한 기능을 가진 평가판본을 설치하거나 가동시킬수 없다. 전자우편주소 sale @ checkpoint.com 으로부터 이 열쇠를 받을수 있다. 사용자차림표는 CD-ROM에서 FireWall-1/Docs/Userguid등록부에 있다. Gs.pdf파일을 열고 《Check Point FireWall-1의 시작》에서 설치와 관련한 내용들을 참고할수 있다.

주 의

Acrobat Reader가 없는 경우에는 CD-ROM으로부터 직접 설치할수 있다. FireWall-1/Docs/Pdfread등록부에서 조작체계에 맞는 설치파일을 선택할수 있다.

Windows NT 4.0에서의 설치는 setup.exe파일을 실행한 다음 설치사의 안내에 따라 설치한다.

경 고

현재 봉사를 운영하고 있는 봉사기에 방화벽견본제품을 설치하여서는 안된다. 방화벽견본제품은 현재의 봉사를 제한함으로써 정확한 가입을 방해하거나 또는 다른 목적에 맞게 봉사기를 리용할수 없게 한다.

가디언(Guardian)

CD에는 또한 NetGuard회사에 의하여 30일평가판본으로 제공되는 Guardian방화벽이 포함되여 있다. Netguard등록부에서 setup.exe파일을 기동하여 프로그람을 설치한다. 설치와 동작에 관한 정보들은 CD-ROM에 PDF형식으로 보관되여 있는 사용자안내서를 참고하시오.

경 고

현재 봉사를 운영하고 있는 봉사기에 방화벽견본제품을 설치하여서는 안된다. 현재의 봉사를 제한함으로써 정확한 가입을 방해하거나 또는 다른 목적에 맞게 봉사기를 리용할수 없게 한다.

Guardian방화벽과 관련한 더 자세한 정보들은 NetGuard회사와 상담하여야 한다.

- NetGuard.Inc
- 2445 Midway Road
- Building 2
- Carrollton.Texas 75006
- 972-738-6900
- sales @ netguard.com
- www.netguard.com

인터네트스캐너(Internet Scanner)

인터네트보안체계(ISS)회사는 자기의 완전한 망보안취약성검사체계인 Internet Scanner에 대하여 제품의 완전한 실행을 위하여서는 암호화된 사용권열쇠를 리용할것을 요구한다.

주 의

ISS로부터 확장된 평가판열쇠를 얻기 위하여서는 ISS회사에 전자우편주소 sales @ iis.net로 요구문서를 보내야 한다. 전자우편에는 이름과 전자우편주소, 우편봉사기주소, 전화번호, 망의 IP주소범위 등을 포함하여야 한다. 허용되면 ISS에 의하여 사용권열쇠가 전자우편으로 주어 진다. 또는 전화번호(888)901-7477로 ISS와 상담할수도 있다.

망감시프로그람묶음(NMS)

CD에는 Lanware회사가 30일평가판본으로 제공한 Network Monitoring Suite(NMS)가 포함되여 있다. NMS는 경로기, 집선기, Windows NT워크스테이션, Windows NT봉사기, UNIX봉사기들로 구성된 망에서 중요한 요소들의 성능을 감시하기 위한 목적으로 설계된 쏘프트웨어프로그람묶음이다.

Web페지 www.lanware.net/download/eval/nms_registration.asp에 신청하여 NMS의 30일사용권을 받을수 있다.

CD의 Lanware등록부에서 setup.exe파일을 실행하여 프로그람들을 설치할수 있다. 설치와 조작에 관한 더 자세한 정보를 얻기 위하여서는 Lanware회사와 상담하여야 한다.

- Lanware, Inc
- Sales @ lanware.net
- www.lanware.net

WinZip

CD에는 Winzip Computing(이전에는 Nico Mak Computing회사)회사의 압축/해제프로그람인 Winzip시험판이 포함되여 있다.

CD의 Winzip등록부에서 setup.exe파일을 실행시켜 설치한다.

주 의

CD에 포함된 다른 제품들의 설치를 위하여 Winzip가 필요하다.

부 록 2. 망리용방책의 실례

이 부록에서는 일부 망리용방책을 실례를 들어서 설명한다. 그러나 리상적인 망리용방책은 산업수요와 기술갱신과 같은 끊임 없는 순환과정을 거쳐서만 완성될수 있다.

주 의

다음의 련결들은 실제의 망리용방책에 대한 두가지 실례이다. 하나는 회사이고 다른 하나는 교육기관이다.

www.dmtnet.com/Internetpolicy/policy.pdf

www.oit.gatech.edu/security/policy/usage/contents.html

효과적인 망리용방책의 원리

망리용방책을 평가하는데서 전통적으로 리용되는 2개의 원리는 다음과 같다.

소유총비용(TCO)

TCO는 생산성과 자원리용의 비로 측정된다.

생산성 망은 정보이동을 쉽게 하여 생산성을 높이기 위하여 존재한다. 리론적으로 이 생산성은 기업관리가 적당한 망리용과 높은 생산성을 담보할수 있도록 진행되고 있는가에 따라 측정된다.

자원리용 회사안의 자원리용은 합리적이여야 한다. 회사에 손해를 주는 망동작은 비용측면에서 합리적이라고 볼수 없다. 망리용방책은 자원리용에서 합리적인 망동작들을 정의함으로써 기타 불필요한 다른 망동작들은 자동적으로 금지시킬수 있어야 한다.

위험경감

보안방책은 회사의 법적책임을 리치에 맞지 않게 손상시키거나 기밀정보를 침해하는것 또는 기관의 부정공개와 같은 망동작들을 정의함으로써 정보활동의 위협을 감소시킨다.

법적책임 각종 차별을 고려한 이러한 정보들은 확장되여 회사에 법적책임을 지우는 다른 통신들을 포함한다.

기밀정보 경쟁대상에게 리익을 주는 정보들을 말한다. 경쟁자들이 맹렬히 조사하는 분야의 정보들이 여기에 포함된다.

인기저락 기관에 대한 부정적인 영상을 줄수 있는 통신 또는 자원리용은 수출감소와 수입감소를 초래하여 기관의 기업활동에 직접 영향을 미친다.

개 발 과 정

특정기관에서의 세부조정을 위한 처리는 다음의 단계들을 거치게 된다.

조건분석 첫 단계는 망을 리용하는 기관에서 모든 부서들의 자료조사에 의하여 실행된다. 이것은 포괄적인 방책을 세울수 있게 할뿐아니라 직원들의 정보지원과 교육을 쉽게 할수 있게 한다.

- 회사의 어느 부서(또는 개인)가 어떤 형태의 망접근을 필요로 하는가?
- 그들이 필요로 하는 망봉사는 무엇인가?
- 현재의 접근방법(시간과 위치를 포함하여)은 어떠한가?
- 어떤 응용프로그람들이 인터네트와 통합되여야 하는가?
- 기밀자료는 무엇으로 구성되는가?
- 측정할수 있는 생산성지표는 무엇이며 망자원을 어떻게 리용하여 이 지표들을 달성하는가?
- 망자원에 대하여 있을수 있는 위험들은 무엇인가?(실례로 회사에 대한 정탐활동, 법적책임, 부정공개)
- 직원감시와 개인비밀을 둘러 싸고 벌어 지는 법적인 론쟁점들은 무엇인가?

정의 두번째 단계에서는 보안방책을 만들기 위하여 첫번째 단계에서 수집한 정보들을 종합한다. 내용은 다음과 같다.

- 전체 회사의 관점/사명, 핵심기업처리/응용프로그람, 개인/집단의 역할에 맞게 접수할수 있는 리용들을 정의한다.
- 기밀자료, 처리, 자원의 정의와 실례
- 회사에 대한 정탐활동, 법적책임, 부정공개를 포함하여 자료에 대한 위험
- 적당한 비밀통신과 직원승인절차의 정의와 실례, 그와 함께 종업원들의 통신을 감시한다는 취지의 선포
- 벌금처리와 항의처리를 포함한 보안방책위반의 결과
- 보안방책에 대한 의견제기와 수정절차
- 보안방책의 보급방법

실현 세번째 단계는 보안방책의 실현이다. 실현은 크게 두 단계로 구성된다.

- 보안방책의 보급과 종업원들에 대한 교육
- 보안방책의 실시

조사 마지막 단계는 보안방책의 기준으로 되는 두가지 원리 즉 소유총비용과 위험경감에 대한 보안방책의 효과성을 조사하는것이다. 만일 보안방책이 이

원리들을 만족시키지 못한다면 개발과정을 다시 반복한다.

Fubar회사에서 개발한 보안방책의 실례를 보기로 하자. Fubar는 여러가지 탁상응용프로그람들을 개발하고 있다. 대표적인 프로그람들로서는 회의일정계획을 세우는 FuMeeting과 직원자료기지체계인 FuHR이다. 회사의 기본청사는 뉴욕에 있으며 작은 판매점들이 싼띠아고에 있다. 이 판매점들은 128K프레임중계련결을 통하여 기본청사에 련결된다. 회사는 또한 인터네트와 T1련결로 결합되여 있다.

회사에서 근무하는 직원들은 200명이상이며 절반이상이 프로그람작성자들이다. Fubar는 매우 현대적인 원격처리보안방책을 가지고 있으며 매 프로그람작성자들은 매주 하루씩 집에서 작업할수 있게 되여 있다. Fubar의 판매점직원들은 제품광고를 하고 전화련계를 가지면서 대부분의 시간을 로상에서 보낸다. 많은 직원들이 자기의 사무실을 떠나서 작업하기때문에 Fubar는 2개의 원격접근방법을 배비하였다. 원격접근은 모뎀풀을 리용한 전화가입과 특정한 VPN쏘프트웨어를 리용한 인터네트련결로 제공된다.

원격련결을 통하여 망에 입력된 정보의 기밀성은 정확히 조정된다. 프로그람작성자들이 최신프로그람코드와 작업하기때문에 이러한 정보가 경쟁대상의 손에 들어 가면 Fubar는 큰 손실을 보게 된다. 판매점정보는 기밀로 처리한다. 그것은 새로운 제품출하에 대한 정보가 경쟁대상들의 손에 들어 갈수 있기때문이다.

범 위

이 문서의 유효범위는 정확한 망리용에 대한 회사들의 보안방책을 정의할 때이다. 회사망에는 리윤률을 지향한 신용 있는 투자가 동반된다. 망은 생산성을 높이고 작업흐름의 효과성을 높이기 위하여 설치된다. 망의 요소들은 다음과 같다.

- 음성과 정보를 나르는 모든 케블
- 음성과 정보의 흐름을 조종하는 모든 장치
- 감시기, 틀, 기억장치, 모뎀, 망기판, 기억소편, 건반, 마우스, 망기판, 케블을 포함한 모든 콤퓨터요소들
- 모든 콤퓨터쏘프트웨어
- 인쇄기와 팍스장치를 포함한 모든 출력장치

이 문서에서 서술한 보안지침을 준수하도록 하기 위하여 범할수 있는 결함에 대한 훈련과정이 매 사건을 기준으로 규정되여 있다. 회사는 지역 또는 국가, 련방법이 적용되지 않을 때 또는 재정손실을 입었을 때 법적문제를 수사할수 있는 권한을 가진다.

망 관 리

탁상체계의 구성변경을 포함하여 망의 모든 유지는 관리성원들에 의하여 유일적으로 진행된다. 관리성원이 아닌 직원들은 체계변경과 지어는 자기의 워크스테이션에 대하여서도 변경을 할수 없다. 다음의 동작들이 체계변경에 영향을 준다.

- 새로운 위치로 옮기면서 체계의 망기능을 변경
- 플로피디스크구동기를 리용하여 체계를 다른 조작체계로 기동
- 체계의 틀 또는 씌우개의 해제
- 인터네트에서 내리적재한 쏘프트웨어를 포함하여 쏘프트웨어묶음의 설치

사용자의 부주의로 인하여 보증이 무효로 되거나 고의적으로 보안예방책을 우회하려는 시도를 제한하기 위하여 하드웨어관리를 제한한다. 쏘프트웨어사용권에 대한 법을 준수하도록 하기 위하여 쏘프트웨어설치를 제한한다. 이러한 대책은 내부관리진영에 의하여 제공된 쏘프트웨어자원만을 리용하도록 함으로써 쏘프트웨어의 비호환성문제를 피할수 있게 한다.

통과암호에 대한 요구사항

매 직원들에게는 망자원에 접근할수 있는 고유한 가입등록이름이 부여된다. 매 가입등록이름은 또한 통과암호와 결합되여야 한다.

통과암호는 권한이 부여된 사용자가 고유한 가입등록이름을 가지고 망자원에 접근한다는것을 확인할수 있게 한다. 자기의 통과암호를 비밀로 보존하는것은 매 직원들의 책임에 속한다. 통과암호는 다음의 지침에 따라서 리용되여야 한다.

- 통과암호는 최소한 여섯문자여야 한다.
- 통과암호는 흔히 쓰는 공통적인 단어 또는 직원의 이름, 가입등록이름, 봉사기이름, 회사이름과 류사하게 구성할수 없다.
- 직원들은 60일에 한번씩 자기의 통과암호를 변경시켜야 한다. 이렇게 하지 않을 때에는 통과암호를 무효화시킨다. 무효구좌를 다시 유효로 하는것은 망관리진영과 접촉할수 있는 자기의 직속관리자에 의하여서만 진행된다.
- 인증할 때 직원들은 3번이내에 자기의 정확한 통과암호를 입력하여야 한다. 3번의 가입시도가 모두 실패한 경우 구좌는 무효화된다. 이렇게 무효화된 구좌를 다시 복귀하는것은 망관리진영과 접촉하는 자기의 직속관리자에 의하여 진행된다.
- 회사안의 모든 콤퓨터는 15min이상 비활동상태이면 동작하는 화면보호기를 리용하여야 한다. 일단 화면보호기가 동작하면 사용자는 가입이름과 통과암호로 다시 가입하여야만 망접근을 할수 잇다.
- 망에 대한 원격접근은 모뎀풀을 리용한 전화가입 또는 인터네트기반 VPN을 통하여 이루어 진다. 이때 직원들에게는 60s마다 새로운 통과암호를 발생하

는 보안통표가 발행된다. 보안통표에 의하여 발생된 통과암호는 직원들이 망에 원격으로 접속할 때 리용된다.

- 통과암호는 비밀로 보관되여야 한다. 직원들은 통과암호를 써놓거나 다른 사람과 공유하지 말아야 한다. 자기의 직속관리자와 인사관리성원에 의하여 통과암호를 넘겨 주어야 하는 경우는 제외된다.
- 회사망의 외부에서 접근할 때에는 내부망에서 리용하던 통과암호와는 다른것을 사용하여야 한다. 이렇게 함으로써 중요한 통과암호문자렬이 다른 망으로 전송되지 않도록 하여야 한다. 회사내부체계에 대한 문제에 대하여서는 자기의 직속관리자 또는 망관리성원에게만 질문할수 있다.
- 회사는 이와 같은 지침에 따라 자기의 통과암호를 비밀로 보존하며 만일 직원이 자기의 잘못으로 인하여 초래되는 손해에 대하여서는 책임지도록 할수 있는 권한을 가진다.

엄격한 통과암호보안방책은 모든 망자원을 안전하게 유지할수 있는 담보를 준다.

비루스예방방책

모든 콤퓨터체계는 반비루스쏘프트웨어에 의하여 보호된다. 자기의 체계에서 동작하는 비루스쏘프트웨어를 발견하는 책임은 직원에게 있다. 체계에서 동작하고 있는 반비루스쏘프트웨어에 의하여 어떤 류형의 경고가 울리면 직원은 즉시에 체계리용을 중지하고 망관리성원 또는 자기의 직속관리자와 상담하여야 한다.

최근의 반비루스쏘프트웨어를 유지하는 책임은 망관리진영성원들에게 있다. 이 프로그람은 직원이 망에 련결되는 기간 자동적인 처리로 실행된다. 자기의 반비루스쏘프트웨어가 60일동안에 한번도 갱신되지 않은 경우 직원들은 망관리성원들에게 제기하여야 한다.

워크스테이션여벌복사방책

망관리성원은 한주일을 기준으로 매 직원들의 워크스테이션에 보관된 문서들에 대하여 여벌복사처리를 진행한다. 매 직원들은 매주마다 한번씩 정해 진 날에 워크스테이션의 전원을 켜놓은 상태로 퇴근하여야 한다. 이때 직원들은 체계에서 탈퇴는 하지만 체계의 전원은 켜놓아야 한다. 정확한 자기날자에 체계의 전원을 켜놓은 상태로 두는것은 직원들의 책임이다. 직원들은 자기의 직속관리자와 토론하여 자기에게 어느 날이 배정되였는가를 알아야 한다.

직원들이 사용하는 워크스테이션에서는 C:\My Documents안에 있는 문서들만 여벌로 보관된다. 다른 등록부에 있는 문서들은 제외된다. 직원들은 모든 문서들을 이 등록부에 보관하여야 할 책임을 지닌다. 회사에 의하여 개발된 응용프로그람들은 기정으로 이 등록부의 파일을 보관하도록 설계된다.

원격망접근

회사는 망자원에 대한 원격련결을 위하여 전화가입모뎀풀들과 인터네트기반VPN을 제공한다. 이것은 원격망접근을 위하여 유일하게 허용된 방법들이다. 탁상체계를 비롯하여 망의 임의의 부분에 모뎀을 리용하여 전화회선과 련결하는것은 엄격히 금지되여 있으며 즉시 해고될수 있는 전제로 된다.

원격망접근은 필요한 경우에만 제공한다. 망자원에 대한 원격접근을 요구하는 직원은 자기의 직속관리자를 통하여 망관리부서에 요구문건을 보내야 한다. 그러면 직원들에게 다음의 정보들이 제공된다.

- 망자원접근을 위한 보안통표
- 모뎀풀전화번호목록
- 인터네트우에서 암호화된 VPN대화를 창조하기 위하여 요구되는 쏘프트웨어
- VPN쏘프트웨어를 설치하는 방향
- 망에 원격으로 접근하는 방향

회사는 망체계가 직원들의 원격접근리용계획을 지원하여야 한다는 책임은 지지 않는다. 직원들은 쏘프트웨어를 접수하고 원격접근을 지원하는데 필요한 모든 갱신을 진행하고 그것에 대한 책임을 지는데 동의해야 한다. 여기에는 꼭 제한되지는 않지만 다음의 요소들이 포함된다.

- 전화회선
- 모뎀
- 고속처리기
- 추가적인 디스크구동기공간

원격접근에 대한 지원은 망관리진영에 의하여 망주변까지를 포함한 망내부에 대하여서만 제공된다. 직원들은 이 유효범위밖에 대한 련결상문제들에 대하여서는 자기자체가 지원할 책임을 지닌다.

직원들은 원격망접근과 관련한 모든 정보들을 비밀로 한다는데 동의한다. 직원들은 통과암호정보를 로출시키지 않는다. 또한 VPN쏘프트웨어의 복사본을 만들지 않으며 지어 다른 직원들을 위하여서도 복사본을 만들수 없다. 원격접근과 관련한 세부정보들을 전파하는것은 보안위반으로서 즉시에 해고될수 있는 전제로 된다.

일반적인 인터네트접근방책

인터네트기반싸이트에 대한 접근을 위하여 리용되는 자원을 포함하여 회사의 모든 망자원은 공적인 작업과 관련한 의무를 수행한다는 명백한 목적에서만 리용된다. 모든 직원들에게 꼭같이 적용되는 이러한 접근방책은 망관련자원의 효과적인 리용을 담보한다. 직속관리자는 이러한 접근방책의 유효범위밖에서의 망자원리용이 다음의 조건에 맞을 때 옳다고 인정한다.

- 망자원의 의도적인 리용은 허용된다.
- 망자원의 의도적인 리용은 직원의 합법적인 의무수행을 방해하지 않는다.
- 망자원의 의도적인 리용은 합법적인 회사관련사업을 위하여 필요하다.
- 망자원의 의도적인 리용은 교육목적을 위하여 필요하며 직원의 직업기능의 유효범위안에서 진행된다.
- 망자원의 의도적인 리용은 지역 또는 국가, 련방법에 위반되지 말아야 한다.
- 망자원의 의도적인 리용은 망의 과부하를 초래해서는 안된다.

인터네트Web싸이트접근방책

인터네트Web싸이트에 접근할 때 직원들은 회사표준에 맞는 Web열람기를 리용하여야 한다. 이 표준은 다음의 구성을 가진 Internet Explorer 5.5의 사용을 요구한다.

- 추가적인 기능추가가 없다.
- Java, JavaScript, ActiveX는 지원되지 않는다.
- Cookie는 지원되지 않는다.

이 설정은 직원들이 인터네트Web봉사기를 방문할 때 부주의로 부당한 응용프로그람들이 적재될수 없게 한다. 이 보안설정에 부합되지 않는 경우에는 인터네트접근권한을 박탈한다. Web열람기는 오직 망관리담당자에 의해서만 설치되여야 한다. 정확한 쏘프트웨어사용권을 유지하기 위하여서는 직원들이 열람기쏘프트웨어를 검색하거나 다른 자원으로부터 갱신하는것을 금지해야 한다. 자기의 열람기가 회사표준과 맞는가를 확인할수 없는 경우에는 망관리자들과 상담하여야 한다.

인터네트우편과 뉴스그룹접근방책

내부와 외부에로의 인터네트우편통보문은 8MB로 최대크기가 제한된다. 이 요구를 초과하는 파일을 전송하려는 경우에는 망관리자들과 상담하여 회사의 FTP봉사기를 리용하여야 한다. 이 제한은 큰 전자우편통보문이 모든 회사통보문들의 흐름에 영향을 미치지 않도록 하기 위하여 실시된다.

인터네트우편목록 또는 뉴스그룹에 전송되는 모든 통보문들에는 회사부인성명을 포함시켜야 한다. 부인성명은 《이 통보문에 반영된 견해는 회사측의 관점을 반영하지 않는다.》이다.

회사는 이러한 전송을 감시하며 이 부인성명을 포함하지 않은 통보문을 페기할수 있는 권한을 가진다.

개인의 인터네트구좌

회사의 망자원은 개인의 인터네트구좌에 접근하는데 리용되지 않는다. 여기에는 다음의 구좌들이 포함된다.

• 개인의 전자우편구좌
• 개인의 쉘구좌
• AOL 또는 CompuServe와 같은 봉사제공자를 가진 개인구좌

직결봉사에 있는 개인구좌는 회사체계로부터 접근될수 없다. 또한 인터네트체계에 존재하는 회사구좌 또는 서명들을 포함할수 없다. 회사구좌에 대한 접근은 접수할수 있는가를 고려한다. 즉 접근이 직원들의 직업적의무와 관련될 때에만 제공된다.

비밀과 경과기록

회사의 모든 망자원은 오직 회사자체의 소유라는것이 회사의 립장이다. 제한되지는 않지만 여기에는 전자우편통보문과 보관된 파일, 망전송 등이 포함된다. 회사는 모든 망동작을 감시하고 경과를 기록할수 있는 권한을 가진다. 직원들은 자기의 직속관리자 또는 인사관리성원들이 요구할 때에만 통과암호와 파일, 다른 요구자원들을 넘겨 줄수 있다.

추 가 정 보

이 문서안의 정보와 관련한 질문과 특별히 설명하지 않은 문제점들에 대하여서는 자기의 중계관리자에게 제기하여야 한다. 중계관리자는 모든 질문들을 망관리부서와 인사관리부서, 기타 적당한 대방들에 중계할 책임을 지닌다.

색 인

ㄱ

가는망케블고장(Thinnet cabling failures) 344
가로채기(hijacking) 275, 391
가벼운 등록부접근규약[Lightweight Directory Access Protocol (LDAP)] 163
가상국부망[virtual local area network(VLAN)] 118
가상기억(virtual memory) 377
가상사설망[Virtual Private Network(VPN)] 162, 294
가입(Login) 382
가입기발(Logon banner) 442
가입데몬[login daemon(UNIX)] 480, 481
가입시간제한화면[Login Time Restrictions screen (NetWare)] 383
가입제한단추[Logon Restrictions button(NetWare)] 383
감시(monitoring) 268
거리벡토르경로조종(distance vector routing) 60
거부명령(deny statements) 180
거울화(mirroring) 343
검사(Testing) 365
검색엔진(search engines) 495
검열(auditing) 389
검열단추[Auditing button(Shared Documents Properties dialog box)] 421
검열도구프로그람[Auditcon(NetWare)] 389
검열합확인(checksum verifications) 333
검열원칙창문[Audit Policy window (Windows NT)] 426
검은모자해커(black hat hackers) 20
경과기록(Logging, logs) 354, 389
경로기(routers) 58
경로기교환(router switching) 122
경로기형VPN(router−based VPN) 302
경로순환고리(routing loop) 66
경로조종(routing) 59
경로조종불가능한 통신규약 (Non−routable protocols) 57
경로조종정보규약[routing information protocol(RIP)] 60
경로조종표(routing tables) 59
고정된 주파수신호(fixed frequency signals) 103
공간전송(space−based transmissions) 103
공격(attacks) 19
공격개시(Launching attacks) 275, 506
공격정보수집(collecting information for attacks) 490
공격징후(attack signatures) 195
공격에 대한 취약성감소(reducing vulnerability to attack) 518
공개/비공개암호열쇠(public/private crypto keys) 281
공개열쇠(public keys) 281
공개열쇠증서봉사(public key certificate services) 447
공개열쇠하부구조[Public Key Infrastructure (Windows PKI)] 448
공개열쇠하부구조봉사[Public Key Infrastructure Service (NetWare PKIS)] 391
공유문서속성대화칸[Shared Documents Properties dialog box (Windows NT)] 417
공유허가대화칸을 통한 접근[Access Through Share Permissions dialog box (Windows NT)] 418
교환기(switches) 116
교환기경로조종(switch routing) 122
구성파일의 보관(saving configuration files) 354
구좌관리(account management) 381

구좌원칙창문[Account Policy window (Windows NT)] 409
굵은망케블고장(Thicknet cabling failures) 344
규칙모임[rule sets(FireWall−1)] 231
규약(protocols) 51
그룹, 집단(groups) 460
그룹성원단추[Group Membership button (NetWare)] 386
그룹식별자[Group ID(GID)] 456
그룹파일[group file(UNIX)] 464
그림자통과암호(shadow passwords) 464
기관증명서권한[Organizational CA (certificate authorities) (NetWare)] 395
기동규약봉사기(bootp server) 477
기동관리자구성(boot manager configuration) 476
기발(flags) 69, 128
기발마당(flag field) 128
기정사용자속성창문[Default User Properties windows (Windows NT)] 415
기정콤퓨터속성창문[Default Computer Properties windows (Windows NT)] 416
기억기상주형비루스스캐너(memory−resident virus scanners) 336, 339
개량암호화규격[Advanced Encryption Standard(AES)] 286
개인의 인터네트구좌(personal Internet−based accounts) 547
계승권한마스크[inherited rights mask (NetWare)] 387
계층−3교환(Layer−3 swiching) 122
계층2련결규약[L2TP(Layer Two Tunneling Protocol)] 288
과정감시(process monitoring) 333
관리자대화칸[Administrators dialog box(FireWall−1)] 218
관문(gateways) 58
광지역망(wide area networks) 108
광지역망의 위상구조[WAN(wide area network) topologies] 108

ㄴ

높은 급의 공격(high−profile attacks) 24
눈물방울공격(teardrop attacks) 242
뉴스그룹(Newsgroups) 547
뉴스봉사기[UNIX][News server(UNIX)] 481
능동등록부(Active Directory) 449
내부공격(internal attacks) 248

ㄷ

다중문자렬편집기[Multi−String Editor (Windows NT)] 439
다중정보계산체계[Multiplex Information Computing System(MULTICS)] 453
다원비루스(multi−partite viruses) 323
단순망관리규약(Simple Network Management Protocol) 93
단순우편전송규약[Simple Mail Transfer Protocol (SMTP)] 92
단일고장점(single points of failure) 352
도약(hops) 58
동적접근목록(dynamic access lists) 190
동적주소변환(dynamic address translation) 201
동적파케트려과(dynamic packet filtering) 137
동적호스트구성규약[DHCP(Dynamic Host Configuration Protocol)] 82
등록고(Registry) 211
등록고권한화면[Registry Rights window(Kane Security Abalyst)] 536
등록고편집기[Registry Editor(Windows)] 438
등록부검열창문[Directory Auditing window (Windows NT)] 422
등록부허가대화칸[Directory Permissions dialog box (Windows NT)] 420
디스크거울화(disk mirroring) 358
디스크중복(disk duplexing) 357
디피−헬만인증(Diffie−Hellman authentication) 281

대리자(proxies) 143
대리자의뢰기(proxy clients) 146
대면부속성화면(방화벽−1) [Interface Properties screen(FireWall−1)] 222
대화가로채기(session hijacking) 275
대화층(session layer) 54
데몬(daemons) 152

ㄹ

려과기구성차림표[Filter Configuration menu (NetWare)] 392
려과기정의화면[Define Filter screen(NetWare)] 394
련결상태경로조종(Link state routing) 67
련결상태방법에서 수렴시간(convergence time with link state) 68
련결조종마당(connection control field) 70
렬인쇄기데몬[Line printer daemon(lpd)] 429
령역(domains) 404
령역신뢰(domain trusts) 404
령역조종기(domain controllers) 404
령역이름봉사[Domain Name Services(DNS)] 84
론리적망(Logical networks) 57
리눅스(Linux) 455

ㅁ

마디점주소(Node addresses) 48
마지막가입이름숨기기(hiding last logon name) 443
마크로비루스(macro viruses) 323
마크로웜(macro worms) 330
막기(blocking) 125, 203
말단경과기록(terminal logging) 354
말단통과암호(terminal password) 172
망뉴스전송규약[Network news transfer Protocol (NNTP)] 91
망다리(bridges) 113
망리용방책의 범위(scope of network usage policy) 543
망리용방책의 원리(principles of network usage policy) 541
망봉사(Network services) 74
망수감기화면[Network Sensor screen (RealSecure)] 262
망시간규약[Network Time Protocol(NTP)] 171
망전송(Network transmissions) 197
망정보봉사+[Information Services Plus (NIS+)] 461
망정보의 전파(propagating network information) 60, 67
망조사(probing networks) 496
망주소(Network addresses) 54
망주소변환[NAT(network address translation)] 157
망주소변환장치(NAT devices) 82
망주소제한화면[Network Address Restriction screen(NetWare)] 384
망재난(Network disasters) 344
망층(Network layer) 54
망통신(Network communications) 46
망파일체계[Network file system(NFS)] 90
망파일체계봉사기(NFS server) 482
망련결하드웨어(Networking hardware) 112
머리부(headers) 46, 242
모듈선택창문의 설정[Set Module Options window(UNIX)] 477
목표선택설정창문[Target Options window(Octopus)] 373
무료접근열쇠결정(Oakley Key Determination) 450
무선기술(wireless technologies) 113
무선파(radio waves) 103
무접속형망통신(connectionless network communications) 71
무정전전원[uninterruptible power supply (UPS)] 356
문맥에 기초한 접근조종[context−based

access control(CBAC)] 194
문서화(documenting) 366
물리자원분석(physical resource analysis) 29
물리적접근공격(physical access attacks) 516
물리층(physical layer) 53
매체고장(media failures) 344
매체접근조종주소[MAC(media access control) addresses] 48

ㅂ

바운스싸이트와 스머프공격(Bounce sites and Smurf attacks) 514
반복기(repeaters) 112
반비루스쏘프트웨어(anti-virus software) 322
반사적접근목록(reflexive access lists) 191
반송파수감다중접근충돌검출[Carrier Sense Multiple Access with collision Detection (CSMA/CD)] 106
발견적스캐너(heuristic scanners) 336
방송주소(broadcast address) 48
방화벽관리를 위한 OpenBSD(OpenBSD for firewall administration) 154
방화벽(firewalls) 124
방화벽-1 원칙편집기(FireWall-1 Policy Editor) 219
방화벽-1(FireWall-1) 205
방화벽-1모듈의 고장극복성(fault tolerance of FireWall-1 Modules) 208
방화벽-1을 위한 봉사기관리(Management Server for FireWall-1) 205
방화벽-1에서 제3자의 장치관리(Third-party device management with FireWall-1) 208
방화벽-1의 경고(Alerts for FireWall-1) 223
방화벽-1의 부하균형(Load balancing with FireWall-1) 208
방화벽시험시접속성보안(connectivity security during firewall testing) 212
방화벽조수우편목록(Firewall-Wizards mailing list) 529
방화벽을 위한 제3자의 도구(third-party tools for firewalls) 164
방화벽형VPN(firewall-based VPN) 302
방화벽의 플래트홈(platforms for firewalls) 149
버클리인터네트이름령역봉사기 [BIND(Berkeley Internet Name Domain) server] 487
별형위상구조(star topology) 349
보기(viewing) 422
보안(security) 19
보안검열창문의 기동[Run Security Audit window(Kane Security Analyst)] 532
보안결점취약성자료기지(Security Bugware vulnerability databases) 526
보안구좌관리자[Security Account Manager (SAM)] 408
보안관련뉴스그룹(security-related newsgroups) 524
보안등가단추[Security Equal to button (NetWare)] 386
보안봉사기(security servers) 206
보안분석기(Security Analyzer) 505
보안식별자[SIDs(Security Identifiers)] 407
보안정돈표식[security clearance labels (NetWare)] 397
보안조종탁[Secure Console(NetWare)] 398
보안통표(security tokens) 291
보안예산(budgets for security) 35
보안에 대한 외부공격(external attacks on security) 22
보안위험평가(evaluating security risks) 32
보안원칙(security policies) 36
보안원칙집행(enforcing security policies) 39
봉사(services) 75
봉사거부공격[DoS(Denial-of-Service)attacks] 31
봉사기(servers) 355
봉사기형방화벽을 위한 마킨토쉬OS (Macintosh OS for server-based firewalls) 150

봉사기형방화벽(server-based firewalls) 150
봉사기회복(server recovery) 364
봉사포구(service ports) 130
부가처리(Overhead) 99
부분망(subnets) 57
부트규약(bootp(boot protocol)) 82
분산스펙트르신호(spread spectrum signals) 104
분산요소객체모형[DCOM(Distributed Component Object Model)] 438
불복종(Noncompliance) 38
블로크암호(block cipher) 279
비동기전송방식[ATM(asynchronous transfer mode)] 111
비루스(viruses) 319
비루스령역(virus domains) 336
비루스보호(protecting against viruses) 325, 340
비루스복제(replicating viruses) 320
비루스스캐너(virus scanners) 334
비루스잠복을 위한 속성조작(attribute manipulation to conceal viruses) 324
비루스예방원칙(virus prevention policy) 545
비루스의 기동분구복제(boot sector replication of viruses) 322
비루스의 다형성돌연변이(polymorphic mutation of viruses) 326
비루스의 크기(size of viruses) 323
비무장지대(DMZ(demilitarized zone)) 166
비밀열쇠알고리듬(secret key algorithms) 281
비상회복디스크(emergency recovery disks) 408
비속박매체(unbound medium) 103
비속박전송(unbound transmissions) 103
비정상완료[ABENDS(abnormal ends)] 378
비용(costs) 28
비콘(beacon) 348
빛분산과 빛섬유케블(Light dispersion and fiber optic cable) 102
빛섬유케블(fiber optic cable) 101
빛전송(Light transmissions) 103
배비(deploying) 159
배회프로필(roaming profile) 413

ㅅ

사건기록설정창문[Event Log Settings window(Windows NT)] 423
사건보기(Event Viewer) 422
사건보기기록의 원격보기(remote viewing of Event Viewer logs) 424
사건보기에서 경과기록의 자동점검 (automated log review in Event Viewer) 425
사설주소배당(private addressing) 158
사전파일(dictionary files) 463
사용자식별자[User ID(UID)] 456
산업정탐(industrial espionage) 22
상태려과(stateful filtering) 143
상태표(state table) 137
설치경로대화칸[Install Paths dialog box (Octopus)] 369
설치점(mount points) 456
설치원칙대화칸[Install Policy dialog box (FireWall-1)] 240
성능(performance) 210
소유권단추[Ownership button(Shared Documents Properties dialog box)] 422
소유총비용과 망리용방책[total cost of ownership(TCO) and network usage policies] 541
속성설정화면[Properties Setup screen (FireWall-1을 참고)] 233
속이기(hoaxes) 327
속임(거짓)(spoofing) 77
속임수려과기(spoofing filter) 184
수감기속성화면[Sensor Properties screen (RealSecure)] 266
수동적인 취약성검사(manual vulnerability checks) 503
수명시간[time to live(TTL)] 85
수자식종합통신망[ISDN(Integrated Services Digital NetWork) media failures] 351

수자식종합통신망매체고장[Integrated Services Digital Network(ISDN) media failures] 351
수자식증명서봉사기(digital certificate servers) 286
수자통신(digital communications) 98
수정보충과 갱신(patches and updates) 519
순환여유검사[CRC(Cyclic Redundancy Check)] 47
숨은 NAT[hiding NAT(network address translation)] 159
숨겨 진 관리자구좌(hidden administrator accounts) 507
스마트카드(smart cards) 396, 451
스머프공격(Smurf attacks) 202
스텔스와 비루스잠복(stealth and virus concealment) 325
스팸(spamming) 24
시간참조봉사기(time reference server) 482
식별단추[Identification button(NetWare)] 381
실패한 가입시도, 검열(failed logon attempts, auditing) 384
실행가능파일들과 접근조종원칙(executable files and access control policies) 332

ㅈ

자동적인 취약성스캐너(automated vulnerability scanners) 505
자료련결층(data-link layer) 53
자료련결층의 련결식별자[data link connection identifier (DLCI)] 111
자료변환, 이식성(data translation, portability of) 96
자료포구(data port) 79
자료흐름(data streams) 324
자료암호화규격[Data Encryption Standard (DES)] 286
자료여벌복사(data backups) 360
자물쇠-열쇠(Lock-and-Key) 179
자산(assets) 27
잘 알려 진 SID(well-known SID) 407
잘 알려 진 포구(well-known prot) 75
잠복비루스(concealing viruses) 323
쟈바스크립트와 보안위협(Java scripts and security threats) 149
저가격디스크묶음(RAID) [RAID (redundant array of inexpensive disks)] 356
전송(Transmissions.See network transmissions) 49
전송층(Transport layer) 54
전자기간섭[Electromagnetic interference (EMI)] 99
전자우편(e-mail) 24, 29
전체 열쇠조사(exhaustive key search) 283
전체망방송(all-networks broadcast) 121
전화번호발생기(war dialers) 491
전원문제(power problems) 99
점대점통로규약[Point-to-Point Tunneling Protocol (PPTP)] 288
접근가능성(accessibility guidelines) 41
접근권한(access rights) 385
접근조종목록(ACLs(access control lists)) 181
접근조종방책(access control policies) 124
접근조종방책서술자(descriptors for access control policy) 125
접속형통신(connection-oriented communications) 69
접합단위대면부[Attachment Unit Interface (AUI)] 169
정보징후(info signatures) 195
정적경로조종(static routing) 59
정적망주소변환[static NAT(network address translastion)] 159
정적파케트려과(static packet filtering) 127
정적확장접근목록(static extended access lists) 179
조종포기경고(relinquish control alert) 378
주소변환규약[ARP(address resolution protocol)] 49

죽음의 Ping(Ping of death) 250
준비신호(Preamble) 46
중개자공격(man-in-the middle attacks) 507
증명서권한기관[certificate authorities(CA)] 287
증분식자료여벌복사(incremental data backups) 361
지상전송(terrestrial transmissions) 104
지적자원위험분석(intellectual resources risk analysis) 29
지역, 망주소(zones, network address as) 57
집선기, 하브(hubs) 112
재난모의(simulating disasters) 365
재난방지와 회복(disaster prevention and recovery) 343
제3자의 기술정보(third-party technical information) 524
제작자보안정보(vendor security information) 518

ㅊ

차분식자료여벌복사(differential data backups) 362
초기화벡토르[initialization vector(IV)] 280
침입검출체계(IDS) [IDS(Intrusion Detection Systems)] 241
침입검출체계수감기(IDS sensors) 242
침입검출체계조종탁(IDS consoles) 242
침입자차단단추[Intruder lockout button (NetWare)] 384
체계감시화면[System Monitoring screen (Kane Security Analyst)] 535
체계방책편집기(System Policy Editor) 413
취약성스캐너(vulnerability scanners) 503
취약성자료기지(vulnerbility databases) 524
취약성(vulnerability) 503

ㅋ

커버로스(Kerberos) 446
콤퓨터긴급응답기구[CERT(Computer Emergency Response Team)] 527
콤퓨터선택대화칸[Select Computer dialog box (Windows NT)] 424
크래커(cracker) 19
큰 인터네트웜(great Internet worm) 329
클라스터화(Clustering) 360
캐쉬중독(cache poisoning) 277
케블고장(cabling failures) 344
케인보안분석기(Kane security Analyst) 531

ㅌ

탁상체계의 비루스보호(desktop system virus protection) 338
통과암호(passwords) 461
통과암호마당(password field) 462
통과암호크래커(password cracker) 515
통과암호파일[password file(UNIX)] 461
통보문요약인증(message digest authentication) 69
통표(Tokens) 397
통표고리매체고장(Token Ring media failures) 347
투명대리자(Transparent proxies) 146
트로이목마(Trojan horses) 331
특권실행방식(Privileged EXEC mode) 170
테프여벌복사(tape backups) 361

ㅍ

파케트교환(packet swiching) 109, 351
파케트교환망(packet-switched networks) 109, 351
파케트려과(packet filtering) 127
파케트서명(packet signatures) 391, 509
파케트전달려과기화면[Packet Forwarding Filters screen(NetWare)] 393
파케트해신(packet decode) 274
파일감염(file infection) 321

파일과 등록부에 대한 권한[Rights to Files and Directories (NetWare)] 385
파일전송규약(FTP) [FTP(File Transfer Protocol)] 79
파일주사(File Scan) 385
파일체계(file systems) 417
파일체계암호화[Encrypting file System (EFS)] 446
파일허가(file permissions) 417
판도라(Pandora) 400
평균전송단위[Mean Transfer Unit(MTU)] 136
평문통신규약(clear text protocols) 275
평문전송(clear text transmissions) 272
평판(reputation) 33
포구 대 응용프로그람의 넘기기[port-to-application mapping (PAM)] 198
포구(ports) 79
포구번호(port numbers) 74
포구스캐너창문[Port Scanner window (Windows NT)] 435
포구스캔(port scans) 435
포구주소변환[port address translation (PAT)] 160
폭탄(bombs) 326
표준접근목록(standard access lists) 182
표현층(presentation layer) 54
프레임(frames) 46
프레임검사렬[frame check sequence(FCS)] 47
프레임머리부(frame header section) 47
프레임중계기술(frame relay technology) 109
프레임중계매체오유(frame relays media failures) 351
프레임해신(frame decode) 49
피동적감시(passive monitoring) 501
페지파일(page file) 444
페품수집설정(garbage collection setting) 378

ㅎ

하쉬(hash) 290
하쉬통보문인증코드[Hash Message Authentication Code (HMAC)] 450
하이퍼본문전송규약[Hypertext Transfer Protocol (HTTP)] 86
한방향신뢰(one-way trusts) 404
한번쓰기(one-time pad) 279
허가(permissions) 417
허가단추[Permissions button(Shared Documents Properties dialog box)] 417
호스트형침입검출체계(host-based IDS) 250
호전적인 공격(militant attacks on security) 23
흐름암호화(stream cipher) 279
힘내기공격(brute force attacks) 283
해커(hackers) 19
해킹(hacking) 19
핵심부구성자(UNIX) [Kernel Configurator (UNIX)] 476
회복(recovering) 446
회색모자해커(grey hat hackers) 20
회전그룹(Wheel group) 465
흰모자해커(white hat hackers) 20
확장접근목록(extended access lists) 186

ㄲ ㄸ ㅃ ㅆ

꼬임쌍선케블(Twisted pair cabling) 112
떨구기(기동분구비루스를 확산시키는 프로그람)(droppers) 322
뿌리구좌(root account) 466
싸이트선택대화칸[Site Select dialog box (Octopus)] 405
쌍방향신뢰(two-way trusts) 404

ㅇ

안내서(guidelines) 41
안전한 소케트층[Secure Sockets Layer(SSL)] 291

안전한 쉘[Secure Shell(SSH)] 290
안전한 하쉬알고리듬[Secure Hash Algorithm(SHA-1)] 290
암호결함(cipher deficiencies) 283
암호문(ciphertext) 279
암호봉사제공자[CSP(cryptographic services provider)] 258
암호설치화면[Cryptographic Setup screen (RealSecure)] 259
암호학(cryptography) 278
암호화(encryption) 278
암호화속성창문[Encryption Properties window(FireWall-1)] 311
암호화에서 인간오유(human error in encryption) 282
암호열쇠(crypto key) 282
여벌, 여벌복사(backups) 362
여유봉사기(redundant servers) 359
열린체계호상련결참조모형[OSI(Open Systems Interconnection Reference) mode] 52
열쇠(Keys) 278
영구가상회선[permanent virtual circuits (PVCs)] 109
요구형비루스스캐너(on-demand virus scanners) 335
우편국규약[Post Office Protocol(POP)] 87
우편목록기입제거(Unsubscribing to mailing lists) 528
우편목록(mailing lists) 528
우편목록기입(subscribing to mailing lists) 529
웃층의 통신(Upper layer communications) 96
응답대화칸[Response dialog box(RealSecure)] 266
응용프로그람봉사제공자[Application Service Provider(ASP)] 363
응용프로그람준위의 비루스스캐너 (application-level virus scanners) 337
응용층(application layer) 55
응용프로그람넘기기(Application mapping) 198
응용에 기초한 방화벽(appliance-based firewalls) 155
이동통신연구쎈터[Nomad Mobile Research Centre (NMRC)] 392
이름봉사기로부터 지역전송제한(Limiting zone transfers from name servers) 494
이써네트(Ethernet) 46
이써네트통신의 무차별방식(promiscuous mode for Ethernet communications) 107
이써네트프레임에 대한 프레임검사렬 (FCS)[FCS(frame check sequence) for Ethernet frames] 47
이써네트프레임의 자료부(data section of Ethernet frames) 47
인식자원분석(perception resource analysis) 31
인쇄기포구대화칸[Printer Ports dialog box(Windows NT)] 429
인증(authentication) 272
인증을 위한 방법목록(method list for authentication) 202
인터네트규약에서 단순열쇠관리(Simple Key Management for Internet Protocols. See SKIP) 304
인터네트뉴스데몬[InterNetNews daemon (INND)] 481
인터네트데몬[Internet daemon(inetd)] 75
인터네트보안련합과 열쇠관리규약[Internet Security Association and Key Management Protocol (ISAKMP)] 450
인터네트정보봉사기[IIS(Internet Information Server)] 436
인터네트조종통보문규약[ICMP(Internet Control Message Protocol)] 131
인터네트중계담화[Internet Relay Chat(IRC)] 95
인트라네트(intranets) 377
일반파일전송규약봉사기[TFTP(Trivial File Transfer Protocol) server] 355
임대선(Leased lines) 108
임대주기(Lease period) 83
위상구조적인 보안(Topology security) 98

위험분석(risk analysis) 28
위험분석조사화면[Risk Analysis Survey window (Kane Security Analyst)] 535
위험분석의 목적(goals of risk analysis) 16
위험경감(risk mitigation) 541
의뢰기(clients) 205, 214
완전자료여벌복사(full data backups) 361
완충기넘침공격(buffer overflow attacks) 510
워크스테이션(Workstations) 545
워크스테이션속성화면[Workstation Properties screen(Fire−−Wall−1)] 311
원격망접근(remote network access) 545
원격방화벽(remote firewalls) 311
원격워크스테이션조종(remote workstation controls) 403
원격인증전화가입사용자봉사[RADIUS (Remote Authentication Dial In User Service)] 163
원자징후(atomic signatures) 195
원천경로조종(source routing) 178
원천마디점주소(source node addresses) 49
원천선택창문[Source Options window (Octopus)] 372
원천선택화면[Select Source screen (Octopus)] 371
웜(worms) 328

수 자

3COM제작자정보(3COM vendor information) 518
3중DES(Tripe DES) 286

A

AAA(인증,권한,회계) 172
ActiveX조종자 147
AES(개량암호화규격) 286
AppleTalk지역 58
ARP캐쉬 51
ATM파케트의 토막화와 재조립 111

B

Bwgtraq우편목록 529

C

C2증서 378
C2MYAZZ도구프로그람 277, 508
C2MYAZZ도구프로그람을 위한 Microsoft의 Windows 95 패취 patch 276
CD−ROM 538
CD−ROM의 Guardian평가복사본 539
CD−ROM의 인터네트스캐너평가복사본 539
CD−ROM의 망감시묶음평가복사본 540
Check Point구성도구대화칸 218
Check Point의 방화벽−1 205
Check Point의 방화벽−1에 대한 평가사용권 213
chgrp도구프로그람 460
chmod도구프로그람 459
chown도구프로그람 460
Cisco경로기 168
Cisco경로기를 위한 EXEC방식 170
Cisco경로기에서 TACAS+ 실행 173
Cisco경로기의 TCP차단 192
Cisco경로기의 인증 201
Cisco발견규약 171

D

DNS봉사기 428
DNS중독 277

E

Exec데몬(UNIX) 480

F

FDDI(빛섬유분산자료대면부)고장 347
FDDI의 전2중방식 348
Filtcfg도구프로그람 392

Finger봉사기 478
FIN스캔 130, 501
FreeBSD 454

G

GID그룹식별자 456

H

HTML스크립트와 보안위협 146

I

ICMP 범람 276
IDS를 위한 수감기 247
IDS의 보복수단 248
IMAP4 88
IMAP봉사기(UNIX) 480
Inetcfg도구프로그람 393
Inetd(인터네트데몬) 74
inetd봉사기 483
inetd봉사기의 봉사파일 483
iNetTools도구프로그람 499
InfoSec뉴스우편목록 529
INND데몬 481
IP규약 54
IP보안규약 449
IP봉사 427
IP속임수 183, 472
IP주소 78
IP포구 74
IP우의 NetBIOS 92
IRC웜 330

L

LophtWeb싸이트 527
Land공격파케트 183
Legato Octopus 366
LPR포구 429
Lucent방화벽화면 267

M

make구성화면 470
make지령 468
MD5 290
Microsoft의 인터네트정보봉사기[Microsoft Internet Information Server(IIS)] 428
Microsoft의 윈도우즈인터네트 이름봉사 [Microsoft Windows Internte Name Service(WINS)] 432
MTU(평균전송단위) 136

N

NetWare 377
NetWare등록부봉사 379
NetWare등록부봉사나무 379
NetWare보안의 세부변경 397
NetWare에서 원격조종탁접근 398
NetWare의 공개열쇠하부구조봉사 395
NMAS를 위한 인체정보인증 396
NMAs의 물리적인증방법 396
Novell 모듈인증봉사 395
nslookup지령 492
NTBugtraq 우편목록 530

O

Octopus 366
Octopus조종탁화면(Octopus console screen) 370
OSI모형의 층 52
OSPF경로조종규약 66

P

passfilt.dll파일[passfilt.dll file 411
Phrack잡지홈페지 528
Ping스캔 498
POP(우편규약) 87

POP3봉사기 273
POP3의뢰기 273
POSIX 456

R

R지령(R commands 480
RealSecure 조종탁화면 254
RealSecure의 설정계획 254
RealSocure에서 보안강화 260
RSA암호화 289

S

SECURE.NCF스크립트 397
Sendmail(UNIX) 481
SKIP속성화면 309
SAMBA 482
SMTP보안봉사기 218
SMTP정의대화칸 219
Sun Microsystems제작자정보 523
SYN공격 234

T

T1선 126
TCP3-파케트련결신호 70
TCP/IP파케트류형화면의 정의 394
TCP/IP규약 393
TCP/IP보안화면 433
TCP기발마당 127
TCP부분주사 501
TCP포장기 488
telnet 69
traceroute지령 496

U

UDP련결 73
UDP머리부해신 131
UNIX통과암호해득 462
UNIX 453
UNIX핵심부의 최적화 467
UNIX핵심부의 콤파일 475
UNIX핵심부의 의존성검사 475
URI정의대화칸 147

V

VPNs의 체계용량 298

W

WANK웜 329
Web싸이트 23
whois지령 94
Windows 2000 445
Windows 2000과 NT에 대한 Octopus 403
Windows NT 402
Windows NT에서 우회횡단검사 412
Windows NT에서 사용자권한 425
Windows NT에서 원격사용자련결해제 410
Windows NT의 DHCP봉사기 427
Windows NT의 공유허가 417
Windows NT의 사용자구좌 403
Windows NT의 프로필 413
Windows NT의 망감시국 429
Windows NT의 망결합규약을 위한 경로조종정보규약 430
Windows NT의 신뢰구조 405
Windows NT의 콤퓨터열람기 427
Windows NT의 원격처리호출구성 431
Windows인터네트이름봉사 432
Windows의 공개열쇠하부구조 448
WinZip 540

X

X.25기술 109
X-Force IDS 토론목록 529
X-Force자료기지 524